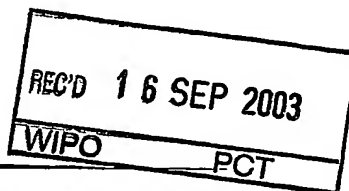


- 2 JUL. 2003



BREVET D'INVENTION

CERTIFICAT D'UTILITÉ - CERTIFICAT D'ADDITION

COPIE OFFICIELLE

CERTIFIED COPY OF
PRIORITY DOCUMENT

Le Directeur général de l'Institut national de la propriété industrielle certifie que le document ci-annexé est la copie certifiée conforme d'une demande de titre de propriété industrielle déposée à l'Institut.

Fait à Paris, le

25 JUIN 2003

Pour le Directeur général de l'Institut
national de la propriété industrielle
Le Chef du Département des brevets

DOCUMENT DE PRIORITÉ

PRÉSENTÉ OU TRANSMIS
CONFORMÉMENT À LA
RÈGLE 17.1.a) OU b)

Martine PLANCHE

BEST AVAILABLE COPY

INSTITUT
NATIONAL DE
LA PROPRIÉTÉ
INDUSTRIELLE

SIEGE
26 bis, rue de Saint Petersburg
75800 PARIS cedex 08
Téléphone : 33 (0)1 53 04 53 04
Télécopie : 33 (0)1 53 04 45 23
www.inpi.fr



INSTITUT
NATIONAL DE
LA PROPRIÉTÉ
INDUSTRIELLE

26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08

Téléphone : 33 (1) 53 04 53 04 Télécopie : 33 (1) 42 94 86 54

BREVET D'INVENTION CERTIFICAT D'UTILITÉ

Code de la propriété intellectuelle - Livre VI



N° 11354*01

REQUÊTE EN DÉLIVRANCE

page 1/2



Cet imprimé est à remplir lisiblement à l'encre noire

DB 540 W / 300301

Réservé à l'INPI

REMISE DES PIÈCES

DATE

26 JUIN 2002

LIEU

75 INPI PARIS

N° D'ENREGISTREMENT

0207954

NATIONAL ATTRIBUÉ PAR L'INPI

DATE DE DÉPÔT ATTRIBUÉE

26 JUIN 2002

PAR L'INPI

Vos références pour ce dossier

(facultatif)

BFF 01/0499

NOM ET ADRESSE DU DEMANDEUR OU DU MANDATAIRE À QUI LA CORRESPONDANCE DOIT ÊTRE ADRESSÉE

CABINET LAVOIX

2, Place d'Estienne d'Orves

75441 PARIS CEDEX 09

Confirmation d'un dépôt par télécopie

☐ N° attribué par l'INPI à la télécopie

2 NATURE DE LA DEMANDE

Cochez l'une des 4 cases suivantes

Demande de brevet

☒

Demande de certificat d'utilité

☐

Demande divisionnaire

☐

Demande de brevet initiale

N°

Date

ou demande de certificat d'utilité initiale

N°

Date

Transformation d'une demande de

☐

brevet européen *Demande de brevet initiale*

N°

Date

3 TITRE DE L'INVENTION (200 caractères ou espaces maximum)

Protocole d'adaptation du degré d'interactivité entre équipements informatiques
interlocuteurs soumis à un dialogue interactif.

4 DÉCLARATION DE PRIORITÉ

OU REQUÊTE DU BÉNÉFICE DE

LA DATE DE DÉPÔT D'UNE

DEMANDE ANTÉRIEURE FRANÇAISE

Pays ou organisation

Date

N°

Pays ou organisation

Date

N°

Pays ou organisation

Date

N°

☐ S'il y a d'autres priorités, cochez la case et utilisez l'imprimé «Suite»

5 DEMANDEUR

☐ S'il y a d'autres demandeurs, cochez la case et utilisez l'imprimé «Suite»

Nom ou dénomination sociale

VIACCESS

Prénoms

Forme juridique

N° SIREN

Code APE-NAF

Société Anonyme

Adresse

Rue

Les Collines de l'Arche, Tour Opéra C,

Code postal et ville

92057 PARIS LA DEFENSE CEDEX

Pays

FRANCE

Nationalité

Française

N° de téléphone (facultatif)

N° de télécopie (facultatif)

Adresse électronique (facultatif)

Remplir impérativement la 2^{ème} page

Réservé à l'INPI

REMISE DES PIÈCES

DATE

26 JUIN 2002

LIEU

75 INPI PARIS

N° D'ENREGISTREMENT

0207954

NATIONAL ATTRIBUÉ PAR L'INPI

DB 540 W / 3C3301

Vos références pour ce dossier :

(facultatif)

BFF 01/0499

6 MANDATAIRE

Nom

Prénom

Cabinet ou Société

CABINET LAVOIX

N° de pouvoir permanent et/ou
de lien contractuel

Adresse

Rue

2 Place d'Estienne d'Orves

Code postal et ville

75441 PARIS CEDEX 09

N° de téléphone (facultatif)

01 53 20 14 20

N° de télécopie (facultatif)

01 48 74 54 56

Adresse électronique (facultatif)

brevets@cabinet-lavoix.com

7 INVENTEUR (S)

Les inventeurs sont les demandeurs

☐ Oui

☒ Non Dans ce cas fournir une désignation d'inventeur(s) séparée

8 RAPPORT DE RECHERCHE

Uniquement pour une demande de brevet (y compris division et transformation)

Établissement immédiat
ou établissement différé

☒

☐

Paiement échelonné de la redevance

Paiement en deux versements, uniquement pour les personnes physiques

☐ Oui

☐ Non

**9 RÉDUCTION DU TAUX
DES REDEVANCES**

Uniquement pour les personnes physiques

☐ Requête pour la première fois pour cette invention (joindre un avis de non-imposition)

☐ Requête antérieurement à ce dépôt (joindre une copie de la décision d'admission pour cette invention ou indiquer sa référence) :

Si vous avez utilisé l'imprimé «Suite»,
indiquez le nombre de pages jointes

**10 SIGNATURE DU DEMANDEUR
OU DU MANDATAIRE**
(Nom et qualité du signataire)

Ph. BLOT
n° 98-0404

Philippe Blot

VISA DE LA PRÉFECTURE
OU DE L'INPI

[Signature]

L'invention concerne un protocole d'adaptation du degré d'interactivité entre équipements informatiques interlocuteurs, soumis à un dialogue interactif.

Les techniques d'échange d'informations entre terminaux informatiques actuellement mises en œuvre, impliquent, afin d'assurer un haut
5 degré de sécurisation de ces échanges, la mise en œuvre de protocoles d'authentification les plus évolués.

De tels protocoles, en règle générale, permettent d'assurer une certitude quasi parfaite de l'origine des informations reçues en l'absence, toutefois, de l'utilisation de connaissances relatives aux qualités intrinsèques
10 des émetteurs de ces dernières ou du ou des utilisateurs de ces émetteurs.

Tout au plus, certains équipements informatiques, tels que terminal équipé d'un lecteur de carte à microprocesseur et carte à microprocesseur, en particulier terminal de désembrouillage, encore désigné décodeur, et carte associée à ce dernier, sont susceptibles de proposer une adaptation du
15 comportement de l'un des équipements en fonction de qualités spécifiques de l'autre de ces équipements, avec lequel cet équipement entre en relation.

Dans cette situation, seul le terminal est en mesure d'adapter son comportement, vis-à-vis de la carte, lorsqu'il est mis en relation avec une carte en fonction du type de carte connectée.

20 L'adaptation précitée est mise en œuvre à partir de la lecture par le terminal, dans la mémoire de la carte, d'informations spécifiques à la carte.

La présente invention a pour objet de remédier aux inconvénients de la technique antérieure connue, et, en particulier, de permettre une adaptation du comportement d'au moins l'un des équipements par soit l'autorisation, soit
25 l'interdiction ou encore l'autorisation conditionnelle de fonctions internes de chaque équipement en fonction de l'identification de l'équipement qui lui est connecté.

En particulier, un autre objet de la présente invention est la mise en œuvre d'un comportement adaptatif de chaque équipement informatique
30 interconnecté, dans le cadre d'un dialogue interactif, suite à un processus d'authentification réciproque entre équipements informatiques, afin de mettre en œuvre un processus d'intercommunication à haut niveau de sécurité dans l'échange des informations en raison du processus d'authentification réciproque

mis en œuvre, d'une part, et du processus d'adaptation comportemental réciproque, de chaque équipement, d'autre part.

Le protocole d'adaptation du degré d'interactivité entre un équipement informatique interlocuteur et un équipement informatique interlocuteur réciproque d'un ensemble d'équipements interlocuteurs, objet de
5 ~~la présente invention, est mis en œuvre lorsque cet équipement interlocuteur et~~
cet équipement interlocuteur réciproque sont soumis à un dialogue interactif.

Il est remarquable en ce qu'il consiste à inscrire, dans cet équipement interlocuteur, une liste d'identifiants d'équipements interlocuteurs réciproques,
10 inscrire, dans cet équipement interlocuteur, une liste d'identifiants de comportements, ces comportements étant pertinents dans le cadre du dialogue interactif, inscrire, dans cet équipement interlocuteur, au moins une association entre un identifiant d'équipements et un identifiant de comportements.

Lors de la mise en présence d'un équipement interlocuteur et d'un
15 équipement interlocuteur réciproque en vue de l'exécution du dialogue interactif, le protocole objet de la présente invention consiste, en outre, à effectuer une procédure d'authentification entre l'équipement interlocuteur et l'équipement interlocuteur réciproque, et, à rechercher l'identifiant de l'équipement interlocuteur réciproque authentifié dans la liste d'identifiants, lire
20 l'identifiant de comportements associé, appliquer, au niveau de l'équipement interlocuteur, le ou les comportements vis-à-vis de l'équipement interlocuteur réciproque authentifié, ce comportement étant sélectionné en fonction du résultat de la procédure d'authentification et associé à l'identifiant de comportements et à l'identifiant de l'équipement interlocuteur réciproque.

25 L'équipement informatique, conforme à l'objet de la présente invention, comprend un circuit d'entrée/sortie permettant d'assurer la transmission et/ou la réception de messages dans le cadre d'un dialogue interactif avec un autre équipement informatique, un module de calcul relié au circuit d'entrée/sortie, une mémoire vive de travail et au moins une mémoire
30 non volatile programmable.

Il est remarquable en ce qu'il comporte au moins, inscrits en mémoire non volatile, une liste d'identifiants d'équipements informatiques, accessibles par l'intermédiaire du circuit d'entrée/sortie, une liste d'identifiants de

comportements pertinents dans le cadre du dialogue interactif et au moins une association entre un identifiant d'équipements et un identifiant de comportements.

Le protocole et l'équipement informatique objets de la présente invention trouvent application à la sécurisation des transactions en réseau, et, notamment, à des transactions de poste à poste ou multipostes, pour des terminaux constitutifs de ces équipements interconnectés en réseau selon le protocole IP, à des transactions entre terminal lecteur de carte à microprocesseur et carte à microprocesseur, interconnectés selon le protocole ISO 7816 par exemple.

Ils seront mieux compris à la lecture de la description et à l'observation des dessins ci-après, dans lesquels :

- la figure 1 représente, à titre illustratif, un organigramme de mise en œuvre du protocole objet de la présente invention entre un équipement informatique, jouant le rôle d'équipement interlocuteur, et un autre équipement informatique, mis en présence en vue d'exécuter un dialogue interactif, cet autre équipement jouant le rôle, vis-à-vis de cet équipement interlocuteur, d'équipement interlocuteur réciproque préalablement à l'exécution proprement dite de ce dialogue interactif, l'un au moins de ces équipements informatiques réalisant une adaptation du degré d'interactivité de ce dialogue interactif vis-à-vis de cet autre équipement informatique, conformément au protocole objet de la présente invention ;

- la figure 2a représente, à titre illustratif, un organigramme de mise en œuvre du protocole objet de la présente invention entre un équipement informatique, jouant le rôle d'équipement interlocuteur, et un autre équipement informatique, mis en présence en vue d'exécuter un dialogue interactif, cet autre équipement, jouant le rôle, vis-à-vis de cet équipement interlocuteur, d'équipement interlocuteur réciproque préalablement à l'exécution proprement dite de ce dialogue interactif, chacun de ces équipements informatiques réalisant une adaptation du degré d'interactivité de ce dialogue interactif vis-à-vis de cet autre équipement informatique, les adaptations du degré d'interactivité de chaque équipement informatique vis-à-vis de cet autre équipement informatique étant indépendantes, mais liées à l'identité de

l'équipement informatique mis en présence pour exécuter ce dialogue interactif, l'ensemble des équipements informatiques mis en présence exécutant, conformément au protocole objet de la présente invention, une adaptation réciproque de l'interactivité de ce dialogue interactif ;

5 - la figure 2b représente, à titre purement illustratif, un exemple de

mise en œuvre préférentiel non limitatif du protocole objet de la présente invention, dans lequel la procédure d'authentification est une procédure à plus d'un niveau d'authentification, afin de permettre une adaptation des comportements associés à l'équipement interlocuteur et/ou à l'équipement
10 interlocuteur réciproque, en fonction du niveau d'authentification vérifié ;

 - la figure 2c représente, à titre illustratif, un premier exemple, non limitatif, de mise en œuvre de liste d'identifiants d'équipements, de liste d'identifiants de comportements et de liste d'associations entre un identifiant d'équipements et un identifiant de comportements pour un premier équipement
15 informatique, équipement A, et un deuxième équipement informatique, équipement B, l'un de ces équipements informatiques jouant le rôle d'équipement interlocuteur et l'autre de ces équipements informatiques jouant le rôle d'équipement interlocuteur réciproque, le dialogue interactif entre ces équipements informatiques pouvant lui-même, à titre d'exemple non limitatif,
20 être conduit par un protocole IP par exemple ;

 - la figure 2d représente, à titre illustratif, un deuxième exemple, non limitatif, de mise en œuvre de liste d'identifiants d'équipements, de liste d'identifiants de comportements, et de liste d'associations entre un identifiant d'équipements et un identifiant de comportements pour un premier équipement
25 informatique, constitué par un terminal, et un deuxième équipement informatique, constitué par une carte à microprocesseur, le terminal constitutif du premier équipement informatique étant muni d'un dispositif lecteur de carte, le terminal et la carte exécutant le dialogue interactif selon le protocole ISO 7816 par exemple ;

30 - la figure 3a représente, à titre illustratif, un mode particulier de mise en œuvre du protocole objet de la présente invention pour un ensemble d'équipements informatiques interconnectés en réseau, chaque équipement étant susceptible d'exécuter un dialogue interactif avec l'un des autres

équipements informatiques de cet ensemble d'équipements, le protocole objet de la présente invention, tel qu'illustré en figure 2a, étant mis en œuvre par couples d'équipements auxquels la qualité d'interlocuteur respectivement d'interlocuteur réciproque a été attribuée ;

5 - la figure 3b représente, à titre illustratif, un mode particulier de mise en œuvre du protocole objet de la présente invention pour un ensemble d'équipements informatiques, l'un des équipements jouant le rôle d'équipement interlocuteur, tel qu'un terminal, chacun des autres équipements jouant le rôle d'interlocuteur réciproque, tel qu'une carte, vis-à-vis de cet équipement
10 interlocuteur ;

 - la figure 4a représente, à titre illustratif, un autre mode particulier de mise en œuvre du protocole objet de la présente invention pour un ensemble d'équipements informatiques interconnectés en réseau, chaque équipement étant susceptible d'exécuter un dialogue interactif avec l'un des autres
15 équipements informatiques de cet ensemble d'équipements, le protocole objet de la présente invention étant mis en œuvre de manière à appliquer un comportement commun de tout équipement de cet ensemble d'équipements vis-à-vis des autres équipements de cet ensemble d'équipements, le comportement commun pouvant correspondre à une liste résultant d'une
20 opération logique réalisée sur des listes de comportements de l'équipement considéré ;

 - la figure 4b représente, à titre purement illustratif, des exemples de mise en œuvre de liste d'identifiants d'équipements, de liste d'identifiants de comportements et de liste d'associations entre un identifiant d'équipements et
25 un identifiant de comportements pour l'exécution du protocole objet de la présente invention conformément au mode de mise en œuvre de la figure 4a ;

 - les figures 4c et 4d représentent, à titre purement illustratif, un mode de calcul de la liste résultante, intersection de listes d'identifiants de comportements, pour des équipements informatiques connectés en réseau
30 respectivement pour un terminal muni d'un lecteur de carte et de deux cartes distinctes ;

 - les figures 4e et 4f représentent, à titre purement illustratif, un mode de calcul de liste résultante, union de listes d'identifiants de comportements,

pour des équipements informatiques connectés en réseau respectivement pour un terminal muni d'un lecteur de carte et de deux cartes distinctes ;

- la figure 5 représente, à titre illustratif, un autre mode particulier de mise en œuvre du protocole objet de la présente invention pour un ensemble d'équipements informatiques interconnectés en réseau, chaque équipement
5 étant susceptible d'exécuter un dialogue interactif avec l'un des autres équipements informatiques de cet ensemble d'équipements, le protocole objet de la présente invention étant mis en œuvre de manière à appliquer un comportement conjoint de tout équipement de cet ensemble d'équipements vis-
10 à-vis des autres équipements de cet ensemble d'équipements, le comportement conjoint pouvant correspondre à une adaptation de l'interactivité de chaque équipement informatique vis-à-vis du sous-ensemble des autres équipements informatiques de cet ensemble d'équipements informatiques, adaptation selon laquelle le sous-ensemble des autres équipements
15 informatiques est établi, du point de vue de l'interactivité, comme un interlocuteur réciproque unique vis-à-vis de cet équipement informatique.

Une description plus détaillée du protocole d'adaptation du degré d'interactivité entre équipements informatiques objet de la présente invention sera maintenant donnée en liaison avec la figure 1.

20 En référence à la figure précitée, on indique que le protocole objet de l'invention est destiné à être mis en œuvre entre deux ou plusieurs équipements informatiques d'un ensemble d'équipements informatiques.

D'une manière générale, dans le cadre de la mise en œuvre du protocole objet de la présente invention, on indique qu'on désigne par
25 "équipement interlocuteur" tout équipement informatique de cet ensemble d'équipements qui prend l'initiative d'un dialogue interactif avec un autre équipement de cet ensemble d'équipements informatiques. Pour cette raison, l'autre équipement informatique est désigné "équipement interlocuteur réciproque", dans le cadre de ce dialogue interactif.

30 En référence à la figure 1 précitée, on indique que l'équipement A est désigné "équipement interlocuteur" et que l'équipement B est désigné "équipement interlocuteur réciproque" en référence à la définition précédemment mentionnée.

Le protocole objet de la présente invention a, notamment, pour objet de réaliser une adaptation du degré d'interactivité entre l'équipement interlocuteur et l'équipement interlocuteur réciproque précité, lorsque l'équipement interlocuteur et l'équipement interlocuteur réciproque sont soumis
5 au dialogue interactif précédemment mentionné.

En référence à la figure 1, on indique que le protocole objet de l'invention consiste à inscrire, dans l'équipement interlocuteur, une liste d'identifiants d'équipements interlocuteurs réciproques et une liste d'identifiants de comportements, ces comportements étant pertinents dans le cadre du
10 dialogue interactif.

Le protocole objet de l'invention consiste également à inscrire, dans l'équipement interlocuteur, équipement A, au moins une association entre un identifiant d'équipement et un identifiant de comportements. L'association
15 précitée peut elle-même être constituée par une liste d'associations.

La notion de liste d'identifiants d'équipements, telle que la liste d'identifiants d'équipements interlocuteurs réciproques précitée, recouvre toute
20 référence à un équipement unique donné ou à une classe ou ensemble d'équipements défini, par exemple, par une référence de version, de marque de fabrication ou de commercialisation, de certification, d'habilitation ou autre.

Suite aux opérations d'inscription précitées, l'équipement interlocuteur dispose au moins d'un ensemble de listes, liste d'identifiants d'équipements interlocuteurs réciproques, liste d'identifiants de comportements
25 et liste d'association précédemment mentionnées.

On comprend, bien entendu, que les étapes d'inscription de la liste d'identifiants d'équipements interlocuteurs réciproques, de la liste d'identifiants
30 de comportements et de la liste d'associations sont réalisées au moins une fois en vue de la mise en œuvre du protocole objet de la présente invention, et peuvent, bien entendu, être répétées pour réactualiser les identifiants d'équipements et/ou de comportements et la liste d'association entre un identifiant d'équipements et un identifiant de comportements, ainsi qu'il sera décrit ultérieurement.

Les opérations d'inscription sont réalisées de manière sécurisée.

En référence à la figure 1, on indique, à titre d'exemple non limitatif, que l'équipement interlocuteur, équipement A, dispose au moins d'une liste d'identifiants d'équipements interlocuteurs réciproques, la liste L_{ID_A} représentant la pluralité de ces identifiants, cette liste vérifiant la relation :

$$5 \quad L_{ID_A} = [IdB, IdC, \dots, IdF, IdH]$$

où Id_B à Id_H sont réputés désigner chacun un identifiant d'équipements interlocuteurs réciproques.

En outre, l'équipement interlocuteur A dispose d'une liste d'identifiants de comportements, notée L_{C_A} , vérifiant la relation :

$$10 \quad L_{C_A} = [RCA_1, RCA_2, \dots, RCA_k, \dots, RCA_n].$$

Dans la liste d'identifiants des comportements, L_{C_A} , RCA_k désigne un identifiant de comportements spécifiques de l'équipement interlocuteur A vis-à-vis de l'équipement interlocuteur réciproque, l'équipement B.

A titre d'exemple non limitatif, on indique que chaque identifiant de comportements RCA_k peut lui même être formé par une liste de comportements élémentaires encore désignés références de comportement, chaque identifiant de comportements RCA_k vérifiant la relation :

$$RCA_k = [CA_1, CA_2, \dots, CA_p].$$

A titre d'exemple non limitatif, on indique que les comportements élémentaires ou références de comportement CA_p peuvent correspondre à des codes de référence de comportement, ainsi qu'il sera décrit ultérieurement.

Enfin, l'équipement interlocuteur A dispose d'une liste d'associations entre un identifiant d'équipements et un identifiant de comportements, la liste d'associations précitée étant notée L_{IC_A} et vérifiant la relation :

$$25 \quad L_{IC_A} = [[IdB[RCA_1]]; [IdC[RCA_k]]; \dots].$$

La forme de construction ou structure de la liste d'associations n'est pas limitative.

En particulier, à l'observation de la figure 1, on comprendra que, à chaque identifiant IdB , ou IdC , ou autre, est associé un identifiant de comportements, c'est-à-dire le comportement RCA_1 relativement à l'identifiant IdB , le comportement RCA_k relativement à l'identifiant IdC et ainsi de suite.

Compte tenu de l'existence des liste d'identifiants d'équipements, liste d'identifiants de comportements et liste d'associations, le protocole objet de la présente invention consiste, en premier lieu, à effectuer une procédure d'authentification entre l'équipement interlocuteur A et l'équipement interlocuteur réciproque B.

Sur la figure 1, on indique que la procédure d'authentification précitée peut consister, par exemple, de manière classique et connue en tant que telle, suite à l'émission d'une requête de dialogue interactif émise par l'équipement A, équipement interlocuteur, vers l'équipement B, équipement interlocuteur réciproque, à transmettre, de l'équipement interlocuteur réciproque B vers l'équipement interlocuteur A, non seulement l'identifiant IdB de l'équipement interlocuteur réciproque B, mais également des valeurs d'authentification de l'équipement interlocuteur réciproque B vis-à-vis de l'équipement interlocuteur A.

Les valeurs d'authentification précitées sont notées Auth(IdB).

La procédure d'authentification, au niveau de l'équipement interlocuteur A, consiste alors, ainsi que représenté sur la figure 1, à effectuer, en une étape 1, une récupération de l'identifiant IdB de l'équipement interlocuteur réciproque B ainsi, bien entendu, qu'une vérification des valeurs d'authentification Auth(IdB) communiquées par l'équipement interlocuteur réciproque B. La vérification des valeurs d'authentification est notée :

$\mathcal{V}(\text{Auth}(\text{IdB}))$.

L'étape de récupération de l'identifiant IdB et de vérification des valeurs d'authentification Auth(IdB) peut consister, ainsi que représenté en figure 1, à vérifier les valeurs d'authentification Auth(IdB) communiquées par l'équipement interlocuteur réciproque B. Cette étape peut permettre de délivrer un résultat de procédure d'authentification correspondant à différents niveaux d'authentification, ainsi qu'il sera décrit ultérieurement.

Suite à l'étape 1 et après vérification des valeurs d'authentification précitées, le protocole objet de l'invention peut consister, en une étape de test 2, à rechercher l'identifiant de l'équipement interlocuteur réciproque dans la liste d'identifiants d'équipements, c'est-à-dire dans la liste L_{ID_A} précédemment citée.

Sur réponse négative à l'étape de test 2, l'identifiant IdB n'étant pas trouvé dans la liste des identifiants L_{ID_A} par exemple, le protocole objet de l'invention peut consister, en une étape 3, à faire appliquer par l'équipement interlocuteur A, un comportement dit "par défaut" vis-à-vis de l'équipement interlocuteur réciproque B. Le comportement par défaut précité peut
 5 ~~avantageusement être établi et sélectionné en fonction du résultat de la~~
 procédure d'authentification, en particulier, du niveau d'authentification vérifié.

A titre d'exemple non limitatif, on indique que, alors que l'authentification a été établie pour un niveau d'authentification donné, les
 10 valeurs d'authentification $Auth(IdB)$ ayant été vérifiées pour le niveau considéré, le protocole objet de l'invention peut consister à renvoyer une requête de l'équipement interlocuteur A vers l'équipement interlocuteur réciproque B, de façon à ce que ce dernier assure une retransmission de sa valeur d'identifiant d'équipement IdB par exemple. D'autres procédures peuvent être prévues, telle
 15 par exemple que l'attribution, dans le cadre de la seule transaction, d'un identifiant de remplacement associé aux valeurs d'authentification $Auth(IdB)$ et au niveau d'authentification précédemment cités.

Sur réponse positive à l'étape de test 2, les procédures d'authentification et d'identification de l'équipement interlocuteur réciproque B
 20 ayant été satisfaites vis-à-vis de l'équipement interlocuteur A, le protocole objet de l'invention peut consister à récupérer le comportement associé à l'identifiant d'équipements trouvé et au résultat de la procédure d'authentification. Cette opération est réalisée à l'étape 4 sur la figure 1.

L'étape 4 précitée peut alors être suivie d'une étape 5 consistant à
 25 appliquer au niveau de l'équipement interlocuteur A le comportement vis-à-vis de l'équipement interlocuteur réciproque.

En référence à la figure 1, on comprend, par exemple, que, sur réponse positive au test 2 d'appartenance de l'identifiant IdB à la liste des identifiants d'équipements L_{ID_A} , les opérations 4 et 5 peuvent alors être mises
 30 en œuvre par lecture de l'identifiant de comportements. Cette opération est réalisée par sélection du premier membre de liste $[IdB[RCA_1]]$ de la liste d'associations précitée L_{IC_A} et, bien entendu, lecture du comportement retenu, c'est-à-dire l'identifiant de comportements RCA_1 puis lecture des

comportements élémentaires tels que définis par l'identifiant de comportements RCA_1 .

En référence à la figure 1, on indique que le protocole objet de la présente invention permet l'adaptation du degré d'interactivité de l'équipement interlocuteur A vis-à-vis de l'équipement interlocuteur réciproque B.

En particulier, on comprend que ce résultat est atteint grâce à la mise en œuvre des liste d'identifiants d'équipements L_{IDA} , liste d'identifiants de comportements L_{CA} et liste d'associations entre un identifiant d'équipements et un identifiant de comportements L_{ICA} précitées ou par toute structure de données correspondante, autre qu'une liste, permettant la discrimination d'identifiants d'équipements, d'identifiants de comportements et de références de comportement ou comportements élémentaires, ainsi que mentionné précédemment dans la description.

En particulier, on comprend, bien entendu, que tout identifiant de comportements RCA_k constitué par une pluralité de valeurs codées représentatives chacune d'un comportement élémentaire, telle que CA_1 , CA_2 , ..., CA_p , peut être défini en fonction de spécificités fonctionnelles et/ou techniques, c'est-à-dire de capacités réactionnelles de l'équipement interlocuteur réciproque B, dans le cadre du dialogue interactif précédemment cité. C'est en particulier le cas pour chaque valeur de comportement élémentaire codée précitée, lequel peut être adapté aux paramètres technico-fonctionnels de l'équipement interlocuteur réciproque B, voire le cas échéant, aux capacités réactionnelles de l'équipement interlocuteur réciproque B ou même à l'utilisation de ces capacités technico-fonctionnelles par l'utilisateur habilité de l'équipement interlocuteur réciproque B précité.

Dans un exemple de mise en œuvre simplifiée non limitatif, on indique que la liste d'associations L_{ICA} peut être remplacée par une mise en correspondance bi-univoque entre un identifiant d'équipements et un identifiant de comportements par le rang de l'identifiant d'équipements et le rang d'identifiant de comportements dans la liste d'identifiants d'équipements L_{IDA} et la liste d'identifiants de comportements L_{CA} par exemple.

Le protocole objet de la présente invention n'est pas limité à la mise en œuvre d'une adaptation du degré d'interactivité entre un équipement

interlocuteur et un équipement interlocuteur réciproque, ainsi que décrit précédemment avec la figure 1.

Selon un autre aspect particulièrement remarquable du protocole objet de la présente invention, celui-ci permet la mise en œuvre de l'adaptation du degré d'interactivité entre équipement interlocuteur A et équipement interlocuteur réciproque B dans tout ensemble d'équipements informatiques, chacun des équipements interlocuteurs A respectivement équipements interlocuteurs réciproques B mettant en œuvre, de manière sensiblement indépendante, le protocole d'adaptation du degré d'interactivité de l'un vis-à-vis de l'autre équipement interlocuteur, ce qui permet la mise en œuvre d'un protocole d'adaptation réciproque de l'interactivité entre un équipement interlocuteur et un équipement interlocuteur réciproque d'un ensemble d'équipements interlocuteurs soumis à un dialogue interactif, ainsi qu'il sera décrit maintenant en liaison avec la figure 2a.

En conséquence, sur la figure 2a, on a représenté un équipement interlocuteur, l'équipement A, et un équipement interlocuteur réciproque, l'équipement B.

Pour chacun des équipements précités, c'est-à-dire équipement interlocuteur A et équipement interlocuteur réciproque B, le protocole objet de l'invention consiste, bien entendu, à effectuer les étapes d'inscription dans l'équipement interlocuteur A respectivement dans l'équipement interlocuteur réciproque B d'une pluralité d'identifiants d'équipements interlocuteurs réciproques respectivement d'équipements interlocuteurs.

On comprend ainsi que l'équipement interlocuteur A dispose de la liste d'identifiants d'équipements interlocuteurs réciproques L_{ID_A} et que l'équipement interlocuteur réciproque B dispose, de son côté, d'une liste d'identifiants d'équipements interlocuteurs L_{ID_B} .

Le protocole objet de l'invention consiste également à inscrire, dans chaque équipement interlocuteur, équipement A, respectivement dans l'équipement interlocuteur réciproque B, une liste d'identifiants de comportements, les comportements étant pertinents dans le cadre du dialogue interactif.

En référence à la figure 2a, on comprend que l'équipement interlocuteur A comporte la liste de comportements L_{CA} et que l'équipement interlocuteur réciproque B comprend une liste de comportements L_{CB} .

Le protocole objet de l'invention consiste également à inscrire une
 5 liste d'associations entre un identifiant d'équipement et un identifiant de comportements dans chaque équipement interlocuteur A et chaque équipement interlocuteur réciproque B. Dans ces conditions, en référence à la figure 2a, on indique que l'équipement interlocuteur A dispose de la liste d'associations L_{ICA} et que l'équipement interlocuteur réciproque dispose d'une liste
 10 d'associations L_{ICB} .

Pour chaque équipement interlocuteur respectivement interlocuteur réciproque, on rappelle que les identifiants de comportements des listes d'identifiants de comportements L_{CA} et L_{CB} sont notés RCA_k respectivement RCB_h par exemple.

15 Lors de la mise en présence d'un équipement interlocuteur A et d'un équipement interlocuteur réciproque B munis de l'ensemble des listes précitées, en vue de l'exécution du dialogue interactif précédemment mentionné dans la description, le protocole objet de la présente invention consiste à effectuer une procédure d'authentification réciproque entre l'équipement interlocuteur A et
 20 l'équipement interlocuteur réciproque B.

D'une manière générale, on indique que la procédure d'authentification réciproque peut consister, sur requête de l'équipement interlocuteur A d'un dialogue interactif, en :

- la transmission de l'équipement interlocuteur réciproque B vers
 25 l'équipement interlocuteur A de l'identifiant IdB et des valeurs d'authentification $Auth(IdB)$, ainsi que mentionné précédemment dans la description relativement à la mise en œuvre du protocole objet de l'invention décrit en liaison avec la figure 1, et en
- la transmission de l'équipement interlocuteur A vers l'équipement
 30 interlocuteur réciproque B de l'identifiant IdA et des valeurs d'authentification $Auth(IdA)$.

On indique que les opérations de transmission des identifiants et des valeurs d'authentification précitées sont réalisées de manière indépendante, la

transmission de l'identifiant d'équipements IdA et des valeurs d'authentification Auth(IdA), par l'équipement interlocuteur A vers l'équipement interlocuteur réciproque B, pouvant être réalisée soit préalablement à la mise en œuvre de l'étape 1 de récupération et de vérification des valeurs d'authentification
 5 Auth(IdB) de l'équipement interlocuteur réciproque B par l'équipement interlocuteur A, soit postérieurement à cette vérification et conditionnellement à celle-ci.

Dans la première hypothèse, les processus d'authentification sont indépendants et le protocole objet de la présente invention d'adaptation de
 10 l'interactivité de l'équipement interlocuteur A vis-à-vis de l'équipement interlocuteur réciproque B peut être rendu totalement indépendant du protocole d'adaptation de l'interactivité de l'équipement interlocuteur réciproque B vis-à-vis de l'équipement interlocuteur A ou réciproquement.

Suite aux étapes de transmission portant la référence 0 pour chacun
 15 des équipement interlocuteur A respectivement équipement interlocuteur réciproque B, chacun de ces équipements met en œuvre l'étape 1 de récupération de l'identifiant IdB de l'équipement interlocuteur réciproque B, pour l'équipement interlocuteur A, respectivement de l'identifiant IdA de l'équipement interlocuteur A, pour l'équipement interlocuteur réciproque B, et de vérification
 20 d'authentification \forall (Auth(IdB)), \forall (Auth(IdA)) des données d'authentification Auth(IdB) respectivement Auth(IdA) pour l'équipement interlocuteur A respectivement équipement interlocuteur réciproque B.

Suite à l'étape 1 et après vérification des valeurs d'authentification précitées, l'équipement interlocuteur A et l'équipement interlocuteur réciproque
 25 B mettent en œuvre l'étape 2 de vérification d'appartenance de l'identifiant de l'équipement interlocuteur réciproque B respectivement de l'équipement interlocuteur A, c'est-à-dire IdB respectivement IdA, à la liste d'identifiants dont dispose l'équipement interlocuteur A respectivement l'équipement interlocuteur réciproque B.

30 Les tests de l'étape 2 vérifient respectivement les relations :

- IdB \in L_IDA ?
- IdA \in L_IDB ?

Sur réponse négative au test d'appartenance 2, l'équipement interlocuteur A respectivement l'équipement interlocuteur réciproque B peut appeler une procédure 3 de comportement par défaut, laquelle peut correspondre à celle définie précédemment dans la description en liaison avec la figure 1.

Sur réponse positive au test d'appartenance 2, l'équipement interlocuteur A respectivement l'équipement interlocuteur réciproque B peut appeler la procédure 4 de récupération de comportement de l'équipement interlocuteur A vis-à-vis de l'identifiant IdB et de l'équipement interlocuteur réciproque B, respectivement de récupération du comportement de l'équipement interlocuteur réciproque B vis-à-vis de l'identifiant IdA et de l'équipement interlocuteur A, puis, enfin, l'étape 5 d'application du comportement associé à l'équipement interlocuteur réciproque B par l'intermédiaire de l'identifiant d'équipement IdB respectivement à l'équipement interlocuteur A par l'intermédiaire de l'identifiant d'équipement de ce dernier IdA. De même que dans le cas de la figure 1, ces comportements sont associés non seulement à l'identifiant d'équipement correspondant, mais également au niveau d'authentification effectivement vérifié.

On comprend, en particulier, que les étapes 4 de récupération du comportement de l'équipement interlocuteur A, vis-à-vis de l'équipement interlocuteur réciproque B respectivement de comportement de l'équipement interlocuteur réciproque B vis-à-vis de l'équipement interlocuteur A, sont mises en œuvre par identification des identifiants IdB de l'équipement interlocuteur réciproque B respectivement de l'identifiant IdA de l'équipement interlocuteur A et lecture des identifiants de comportements correspondants dans les listes d'associations L_{ICA} respectivement L_{ICB} , ainsi que mentionné précédemment dans la description relativement à la figure 1.

Un mode de mise en œuvre préférentiel non limitatif du protocole objet de la présente invention sera maintenant décrit en liaison avec la figure 2b, dans le cas où la procédure d'authentification entre équipement interlocuteur et équipement interlocuteur réciproque est une procédure à plus d'un niveau d'authentification.

On comprend, en particulier, qu'une telle mise en œuvre permet une adaptation des comportements associés à l'équipement interlocuteur et/ou à l'équipement interlocuteur réciproque en fonction du niveau d'authentification vérifié au cours de la procédure d'authentification mise en œuvre soit selon la figure 1, soit selon la figure 2a.

Sur la figure 2b, les mêmes étapes présentent les mêmes références que dans le cas de la figure 1 ou de la figure 2a.

On considère, en outre, selon l'hypothèse première formulée, que l'équipement A constitue l'équipement interlocuteur et que l'équipement B constitue l'équipement interlocuteur réciproque de manière non limitative.

Dans le mode de mise en œuvre de la figure 2b, on considère que la procédure d'authentification entre équipement interlocuteur A et équipement interlocuteur réciproque B comporte, à titre d'exemple non limitatif, trois niveaux d'authentification, un niveau d'authentification forte, un niveau d'authentification intermédiaire et un niveau d'authentification nulle.

A titre d'exemple non limitatif, on considère que le niveau d'authentification forte correspond à une procédure d'authentification mettant en œuvre, par exemple, des algorithmes de vérification de signature et de déchiffrement particulièrement adaptés, qu'en outre, le niveau d'authentification intermédiaire correspond, par exemple, à l'absence de vérification du niveau d'authentification forte, une procédure d'authentification intermédiaire étant alors introduite, et que le niveau d'authentification nulle correspond à l'absence de vérification du niveau d'authentification forte et du niveau d'authentification intermédiaire, seul l'identifiant IdB de l'équipement interlocuteur réciproque B étant réputé appartenir à la liste des identifiants d'équipements contenue dans l'équipement interlocuteur A par exemple.

En référence à la figure 2b, on observe, à titre d'exemple non limitatif, que l'étape 0 correspondant à l'étape de transmission de l'équipement interlocuteur réciproque B vers l'équipement interlocuteur A de l'identifiant IdB et des valeurs d'authentification Auth(IdB) correspond à une première sous-étape 0₁ de transmission de ces éléments vers l'équipement interlocuteur A.

La sous-étape 0_1 est alors suivie de l'étape 1, de l'étape 2, le cas échéant de l'étape 3, de même que dans le cas de la figure 1 ou de la figure 2a précédemment décrites.

5 A titre d'exemple non limitatif, on indique que l'étape de récupération de l'identifiant IdB de l'équipement interlocuteur réciproque B, puis de vérification des valeurs d'authentification, peut alors être réalisée selon une procédure d'authentification de niveau d'authentification forte, le calcul et la vérification de signature, par exemple au moyen d'algorithmes adaptés, étant réalisés au cours de l'étape 1 précitée.

10 L'étape 1 mentionnée est alors suivie de l'étape 2 de test précitée et de l'étape 3, de même que dans le cas de la figure 1 ou de la figure 2a.

Sur réponse positive au test d'appartenance 2 de l'identifiant IdB à la liste des identifiants L_{ID_A} , alors la procédure d'authentification selon le niveau d'authentification forte peut être engagée.

15 En d'autres termes, l'étape 4 de la figure 1 ou de la figure 2a est appelée en tenant compte de la pluralité de niveaux d'authentification susceptibles d'être vérifiés.

Dans ces conditions, l'étape 4 précitée peut comporter une étape de test 4_1 consistant à vérifier à la valeur vraie le résultat de la vérification de la
20 valeur d'authentification, obtenu suite au calcul de $\mathcal{V}(\text{Auth}(IdB))$ précité.

Sur réponse positive au test de vérification 4_1 précité, le test 4_1 est alors suivi d'une étape 4_2 permettant de récupérer le comportement associé à l'identifiant IdB dans le cadre de la vérification d'un niveau d'authentification forte.

25 L'étape 4_2 précitée est alors suivie de l'étape 5 consistant à appliquer le comportement associé à l'identifiant IdB par l'équipement interlocuteur A, de même que dans le cas des figures 1 ou 2a.

Au contraire, sur réponse négative au test 4_1 , le niveau d'authentification forte n'ayant pas été vérifié, la procédure relative au niveau
30 d'authentification intermédiaire peut être appelée.

Ainsi que représenté en figure 2b, celle-ci peut consister à requérir la présentation d'un code porteur de l'équipement interlocuteur réciproque B, ce code porteur pouvant correspondre au code PIN de l'utilisateur de l'équipement

interlocuteur réciproque B par exemple, à l'étape 0₂ représentée sur la figure 2b.

Le code porteur précité est désigné PIN(ldB). En tout état de cause, il peut consister en une information présente dans la carte ou, le cas échéant, en un code entré au clavier par l'utilisateur par exemple.

L'étape de test 4₁ est alors suivie d'une étape 6₁ de récupération et de vérification du code porteur précité PIN(ldB).

L'étape de vérification peut consister en une étape de test de vérification de la valeur du code porteur précité, vérifiant la relation :

10 - PIN(ldB) correct ?.

Les sous-étapes 6₁ et 6₂ constituent, en fait, une étape 6 correspondant à une étape d'authentification de niveau d'authentification intermédiaire.

Sur réponse positive au test de vérification du code porteur 6₂, l'on procède alors à la récupération du comportement associé à l'identifiant IdB pour le code porteur vérifié précédemment mentionné. Le comportement correspondant récupéré est alors appliqué à l'étape 5.

Au contraire, sur réponse négative à l'étape de test 6₂ précitée, une étape correspondant à un niveau d'authentification nulle est appelée. On rappelle que le niveau d'authentification nulle peut, à titre d'exemple non limitatif, simplement consister en la vérification antérieure de l'appartenance de l'identifiant IdB à la liste des identifiants L_ID_A précédemment mentionnée.

Dans ces conditions, on procède ensuite à la récupération du comportement associé à la valeur de code porteur PIN faux et à l'identifiant IdB de l'équipement interlocuteur réciproque, puis, par retour à l'étape 5, à l'application de ce comportement associé à l'identifiant précité.

Différents exemples de mise en œuvre de listes d'identifiants d'équipements, de listes d'identifiants de comportements et de listes d'associations entre un identifiant d'équipements et un identifiant de comportements seront maintenant donnés en liaison avec les figures 2c et 2d.

Sur la figure 2c, on a représenté les listes précitées attribuées, à titre d'exemple non limitatif, à l'équipement interlocuteur A, les listes précitées étant

réputées identiques à celles attribuées à l'équipement interlocuteur A de la figure 1 afin de ne pas surcharger la notation.

De même, on a représenté sur la même figure 2c les listes correspondantes relatives à l'équipement interlocuteur réciproque B, ces listes vérifiant les relations :

- Listes d'identifiants d'équipements :

- $L_{ID_B} = [IdA, IdD, IdE]$

- Listes d'identifiants de comportements :

- $L_{C_B} = [RCB_1, RCB_2, ..., RCB_h, ..., RCB_r]$

- Identifiant de comportements :

- $RCB_h = [CB_1, CB_2, ..., CB_q]$

- Listes d'associations entre un identifiant d'équipements et un identifiant de comportements :

- $L_{IC_B} = [[IdA[RCB_2]]; [IdD[RCB_1]]]$.

En ce qui concerne la structure des identifiants de comportements RCA_k respectivement RCB_h , on indique que ces derniers peuvent être constitués par une liste comportant au moins un élément constituant une référence de comportement ou comportement élémentaire d'acceptation de dialogue interactif, de refus de dialogue interactif ou d'acceptation conditionnelle de dialogue interactif.

A titre d'exemple non limitatif, on indique que, pour réaliser une telle fonction, chaque liste définissant un identifiant de comportement RCA_k respectivement RCB_h , peut comporter une valeur de comportement élémentaire ou de référence de comportement spécifique, placée par exemple en tête de liste, c'est-à-dire l'élément de tête de liste CA_1 respectivement CB_1 par exemple correspondant à une valeur codée d'acceptation de dialogue interactif, de refus de dialogue interactif ou d'acceptation conditionnelle de dialogue interactif. Les valeurs codées peuvent être quelconques, à chaque valeur codée correspondante étant associé, sur simple lecture, soit l'acceptation de dialogue interactif, soit le refus du dialogue interactif ou encore l'acceptation conditionnelle de ce dialogue interactif.

A titre d'exemple non limitatif, dans le cas où la valeur codée correspond à une valeur codée d'acceptation conditionnelle de dialogue

interactif, la lecture de cette valeur codée en tête de liste permet l'appel d'une fonction des comportements élémentaires ou références de comportements successifs CA_2, \dots, CA_p respectivement CB_2, \dots, CB_q par exemple.

5 D'une manière générale, on indique que les valeurs codées de comportements élémentaires précitées, constitutives des identifiants de comportements RCA_k respectivement RCB_n , peuvent correspondre à des valeurs codées d'appel de primitives de fonctions mises en œuvre par l'équipement interlocuteur A vis-à-vis de l'équipement interlocuteur réciproque B et respectivement de primitives de fonctions de l'équipement interlocuteur
10 réciproque B mises en œuvre vis-à-vis de l'équipement interlocuteur A.

On rappelle que les fonctions précitées désignent les fonctions de chaque équipement, le cas échéant, l'utilisation de telles fonctions par l'utilisateur de chaque équipement, ainsi qu'il sera décrit ultérieurement dans la description.

15 La figure 2d représente des exemples de mise en œuvre des listes précitées dans un cas plus particulier où l'équipement interlocuteur A est constitué par un terminal et où l'équipement interlocuteur réciproque B est constitué par une carte à microprocesseur ou un module logiciel jouant le rôle d'une telle carte vis-à-vis du terminal précité, le terminal étant équipé d'un
20 lecteur de carte et l'échange des données entre le terminal et la carte étant effectué conformément au protocole ISO 7816.

La description des exemples de mise en œuvre des liste d'identifiants d'équipements, liste d'identifiants de comportements, et liste d'associations entre un identifiant d'équipements et un identifiant de comportements sera
25 donnée dans le cas plus particulier non limitatif où l'équipement interlocuteur est constitué par un terminal décodeur et constitue un terminal de désembrouillage d'informations embrouillées et où la carte constitutive de l'équipement interlocuteur réciproque est constituée par une carte dédiée attribuée à tout utilisateur habilité de ce terminal de désembrouillage.

30 Dans une telle application, on rappelle que les informations embrouillées sont transmises en mode point-multipoint par exemple à partir d'un centre d'émission et que l'ensemble équipement interlocuteur A, terminal de désembrouillage, équipement interlocuteur réciproque B, carte à

microprocesseur, permet d'effectuer un contrôle d'accès à ces informations embrouillées.

On rappelle en particulier que le contrôle d'accès à ces informations est effectué à partir de messages de contrôle d'accès, messages ECM, contenant le cryptogramme d'un mot de contrôle et des critères d'accès transmis périodiquement avec les informations embrouillées.

Dans ces conditions, la carte à microprocesseur dédiée joue le rôle de module de contrôle d'accès. Le module de contrôle d'accès comporte au moins un processeur de sécurité et une mémoire non volatile programmable sécurisée comportant des droits d'accès inscrits dans la mémoire non volatile programmable précitée.

La gestion des droits d'accès inscrits est effectuée à partir de messages de gestion de droits d'accès, ces messages étant transmis avec les informations embrouillées.

On rappelle enfin que le contrôle d'accès à ces informations est effectué sur vérification de l'identité d'au moins un droit de contrôle d'accès inscrit dans la carte et d'un des critères d'accès transmis par les messages de contrôle d'accès, cette vérification d'identité étant suivie d'un déchiffrement par l'équipement interlocuteur réciproque, c'est-à-dire par la carte à microprocesseur, du cryptogramme du mot de contrôle à partir d'une clé d'exploitation pour restituer le mot de contrôle d'origine. Le mot de contrôle d'origine est transmis, après déchiffrement par la carte à microprocesseur, c'est-à-dire par l'équipement interlocuteur réciproque B, vers le terminal de désembrouillage, équipement interlocuteur A, pour permettre le désembrouillage des informations embrouillées par ce dernier à partir du mot de contrôle restitué.

Sur la figure 2d, on a représenté, à titre d'exemple non limitatif, les listes L_{ID_A} et L_{C_A} , listes d'identifiants d'équipements et listes d'identifiants de comportements de l'équipement interlocuteur A, c'est-à-dire du terminal de désembrouillage. Ces listes sont réputées identiques à celles décrites en liaison avec la figure 1 afin de ne pas surcharger la notation.

Il en est de même en ce qui concerne l'équipement interlocuteur réciproque B, c'est-à-dire la carte, pour lequel les listes L_{ID_B} et L_{C_B} sont

identiques à celles de l'équipement interlocuteur réciproque B représenté en figure 2c.

Toutefois, en ce qui concerne les comportements identifiés par les identifiants de comportements RCA_k et RCB_h respectifs de l'équipement interlocuteur A et de l'équipement interlocuteur réciproque B, on indique dans
 5 cette situation, que ces derniers et, en raison du mode de mise en œuvre spécifique de l'intercommunication entre l'équipement interlocuteur A et l'équipement interlocuteur réciproque B constitué par la carte, ces comportements présentent une structure spécifique qui est celle d'une chaîne
 10 de bits à la valeur zéro ou un.

Les valeurs indiquées sur la figure 2d sont totalement arbitraires et correspondent à un nombre de bits successifs déterminés, concaténés pour constituer les comportements précitées.

On comprend en particulier que, dans le mode de mise en œuvre
 15 relatif à la figure 2d, c'est-à-dire dans la situation où l'équipement interlocuteur A est un terminal, tel qu'un terminal de désembrouillage, et l'équipement interlocuteur réciproque B est une carte à microprocesseur, chaque bit successif constitutif de la valeur du comportement constitue en fait un comportement élémentaire ou référence de comportement dont la position
 20 correspond aux éléments de liste CA_p respectivement CB_q de la figure 2c pour les mêmes valeurs de comportements identifiés par RCA_k respectivement RCB_h .

On comprend en particulier que, dans le mode de réalisation de la figure 2d, la position de chaque bit dans la chaîne de bits constitutive des
 25 comportements définit en fait un comportement élémentaire ou référence de comportement et la valeur du bit correspondant un ou zéro désigne la mise en œuvre d'une fonction ou l'absence de mise en œuvre d'une fonction correspondante, définissant ce comportement élémentaire ou référence de comportement.

30

Différents exemples de comportements d'un terminal de désembrouillage respectivement d'une carte à microprocesseur associée à ce

dernier, carte d'abonné, seront maintenant donnés en liaison avec la figure 2d précitée.

D'une manière générale, et dans l'application au contrôle d'accès en particulier, une carte à microprocesseur dédiée et attribuée à un abonné est capable de traiter diverses actions, lesquelles peuvent lui être demandées par les messages de gestion transmis au cours du processus de contrôle d'accès. A titre d'exemple, on indique que ces actions comportent, de manière non limitative :

- l'authentification du terminal de désembrouillage,
- inscription/modification d'une clé de service par exemple,
- inscription/modification d'un certificat,
- inscription/modification/effacement d'un droit inscrit dans la mémoire programmable non volatile de la carte,
- consultation d'une donnée interne telle qu'une donnée sécurisée par exemple, valeur d'un titre d'accès ou autre.

L'énumération précédente n'est pas limitative.

Conformément au protocole objet de la présente invention, et en référence à la figure 2d, on indique que la liste des actions ou fonctions mises en œuvre par la carte est alors représentée par la chaîne de bits représentant le comportement identifié par RCB_n tel que représenté en figure 2d.

Si le bit d'une action ou d'une fonction est à la valeur zéro, la carte refuse d'exécuter cette action, s'il est à la valeur un, la carte peut, au contraire, exécuter cette action ou cette fonction.

En ce qui concerne le terminal, celui-ci, de manière semblable, est également capable d'effectuer divers traitements qui lui sont demandés dans les messages de gestion par exemple ou dans le cadre de son dialogue interactif avec la carte à microprocesseur, le terminal de désembrouillage jouant le rôle d'équipement interlocuteur A et la carte à microprocesseur le rôle de l'équipement interlocuteur réciproque B par exemple.

Ainsi, le terminal de désembrouillage est en mesure d'effectuer les opérations ci-après :

- authentification de la carte,
- inscription/modification d'une clé de service dans le terminal,

- inscription/modification d'un certificat,
- transmission des messages de gestion à la carte,
- transmission des messages de contrôle à la carte.

L'énumération précédente n'est pas limitative.

5 De même que dans le cas de l'équipement interlocuteur réciproque,

différents exemples de comportements d'un terminal de désembrouillage et d'une carte à microprocesseur jouant le rôle de module de contrôle d'accès, chacun de ces éléments jouant le rôle d'équipement interlocuteur A respectivement d'équipement interlocuteur réciproque B, seront maintenant
10 donnés ci-après en référence aux éléments de la figure 2d, en particulier des structures de listes précédemment décrites dans la description.

Les exemples précités concernent, en particulier, les étapes de récupération des identifiants, de vérification des valeurs d'authentification, de test à la valeur vraie de ces valeurs d'authentification, d'application d'un
15 comportement associé à l'authentification vérifiée à la valeur fausse, d'application du comportement par défaut, tel que décrit précédemment en liaison avec les figures 1, 2a et 2d.

D'une manière générale, on considère que la notion d'équipement interlocuteur respectivement d'équipement interlocuteur réciproque est
20 interchangeable entre le terminal de désembrouillage et la carte associée à ce dernier. Cette notion d'interchangeabilité est justifiée par le fait que les procédures d'adaptation de l'interactivité peuvent être rendues totalement indépendantes l'une de l'autre.

Ainsi, lorsque la procédure d'authentification du terminal de désembrouillage par la carte n'est pas réussie, c'est-à-dire sur réponse négative au test 2 de la figure 2a pour l'équipement interlocuteur réciproque B par exemple, la carte n'a pas pu procéder à l'authentification du terminal de désembrouillage ou dans le cas où la carte a réussi l'authentification, cette dernière connaît l'identifiant IdA du terminal de désembrouillage.

30 De la même manière, lorsque, suite à la procédure d'authentification de la carte par le terminal de désembrouillage, équipement interlocuteur A, ce dernier n'a pas authentifié la carte équipement interlocuteur réciproque B, ou dans le cas où il l'a authentifiée, ce dernier connaît l'identifiant IdB de la carte,

c'est-à-dire de l'équipement interlocuteur réciproque B. On rappelle que, dans le cas particulier du contrôle d'accès, l'identifiant IdB de la carte peut être constitué par l'adresse unique UA de cette dernière. Chaque élément équipement interlocuteur A, équipement interlocuteur réciproque B, c'est-à-dire terminal et carte, est alors en mesure de sélectionner le comportement à appliquer vis-à-vis de l'autre élément carte, terminal respectivement.

Les exemples de comportement peuvent alors être les suivants :

10 Exemples de comportement de la carte, équipement interlocuteur réciproque.

- Comportement en cas d'échec de l'authentification du terminal par la carte :

15 - Invalidation de toutes les actions de la carte, excepté celles concernant l'authentification du terminal de désembrouillage.

- Comportement lorsque le terminal de désembrouillage a authentifié la carte et n'est pas habilité à conduire un dialogue interactif avec la carte, le terminal étant considéré comme inscrit dans une liste noire :

20 - Invalidation de toutes les actions de la carte, excepté celles concernant l'authentification du terminal.

25 Un tel comportement peut être appliqué par la carte, c'est-à-dire par l'équipement interlocuteur réciproque B, si ce dernier a authentifié le terminal de désembrouillage équipement interlocuteur A et si l'identifiant du terminal IdA est associé à un identifiant de comportements vis-à-vis de terminaux considérés comme inscrits dans une liste noire.

30 On indique, à titre d'exemple non limitatif que, la valeur de comportement spécifique correspond à une chaîne de bits dont tous les bits sont à la valeur zéro, excepté le bit correspondant à l'authentification du terminal de désembrouillage, équipement interlocuteur A.

- Comportement contrôlant l'adaptation, c'est-à-dire l'appariement, de l'interactivité de la carte équipement interlocuteur réciproque B avec un ou plusieurs terminaux de désembrouillage équipement interlocuteur A, le ou les terminaux étant considérés comme inscrits dans la liste des terminaux autorisés :

5

- Toutes les actions de la carte peuvent être autorisées, la sélection des actions ou fonctions validées dans la carte dépendant uniquement des fonctionnalités souhaitées dans le cadre de cet appariement.

10 On comprend, dans cette situation, que la chaîne de bits représentative du comportement, c'est-à-dire la chaîne de bits identifiée par RCB_h , présente une série de valeurs de un et de zéro en fonction des actions ou fonctions de la carte validée.

15 Un tel comportement est appliqué par la carte équipement interlocuteur réciproque B si celui-ci a authentifié le terminal équipement interlocuteur A et si l'identifiant du terminal IdA est dans la liste connue par la carte des terminaux considérés comme inscrits dans la liste des terminaux autorisés, en raison des comportements qui leur sont associés.

20 • Comportement par défaut :

- Ce comportement est appliqué par la carte équipement interlocuteur réciproque B si ce dernier a authentifié le terminal et si l'identifiant de ce terminal, équipement interlocuteur A, et dont l'identifiant correspondant IdA n'est pas dans la liste d'identifiants L_{ID_B} de la carte.

25

En conséquence, aucun comportement spécifique ne peut être sélectionné. Dans cette situation, le comportement par défaut est appliqué.

A titre d'exemple, pour ce comportement par défaut, toutes les actions de la carte interlocuteur réciproque B peuvent être autorisées.

30

- Association du comportement par défaut à l'appariement effectif, c'est-à-dire à la liste d'association de listes L_{IC_B} :

- Invalidation de toutes les actions de la carte, excepté celles concernant l'authentification du terminal de désembrouillage équipement interlocuteur A.

5

Exemples de comportement du terminal de désembrouillage, équipement interlocuteur A.

- Comportement en cas d'échec de l'authentification de la carte par le terminal :
 10 Cette situation correspond à la réponse négative à l'étape de test 2 de la figure 2a pour l'équipement interlocuteur A.
 - Invalidation des traitements comportant des échanges avec la carte, excepté ceux concernant l'authentification de la carte.
- Comportement lorsque la carte, équipement interlocuteur
 15 réciproque B a authentifié le terminal de désembrouillage et n'est pas habilitée à conduire un dialogue interactif avec le terminal, équipement interlocuteur A, la carte étant considérée comme inscrite dans une liste noire :
 20 - Invalidation des traitements comportant des échanges avec la carte, excepté ceux concernant l'authentification de la carte.

Le comportement précité est alors appliqué par le terminal si celui-ci a authentifié la carte et si l'identifiant de la carte, c'est-à-dire l'adresse unique de cette dernière UA, est associé à un identifiant de comportements vis-à-vis de
 25 cartes considérées comme inscrites dans une liste noire.

On comprend que, de même que dans le cas de la carte, dans l'exemple donné précédemment dans la description, le terminal de désembrouillage équipement interlocuteur A peut, bien entendu, disposer d'identifiants de cartes considérées comme inscrites dans une liste noire,
 30 lesquelles, bien qu'habilitées à engager le dialogue interactif, se sont vues retirer la faculté d'engager ce dialogue interactif en raison, notamment, du non respect de contraintes établies pour l'exécution de ce dialogue interactif.

On comprend, en particulier, que ce retrait peut être réalisé lorsque la carte comporte une application de gestion de porte-jetons ou porte-monnaie électronique lors d'une atteinte trop fréquente d'un solde débiteur en nombre de jetons par l'utilisateur de la carte par exemple.

5 Ainsi, selon un aspect particulièrement remarquable du protocole d'adaptation de l'interactivité d'équipement interlocuteur et d'équipement interlocuteur réciproque objet de la présente invention, il est possible non seulement d'adapter le caractère ou le degré d'interactivité et l'interactivité d'équipements communiquant dans le cadre d'un dialogue interactif en fonction
10 de fonctionnalités ou actions de chacun de ces équipements vis-à-vis d'un autre équipement, mais également, le cas échéant, d'une utilisation de ces fonctions ou actions par l'utilisateur de ces derniers.

• Comportement contrôlant l'adaptation ou appariement de
15 l'interactivité d'un terminal de désembrouillage, équipement interlocuteur A, vis-à-vis d'une ou plusieurs cartes équipement interlocuteur réciproque B, la ou les cartes étant considérées comme inscrites dans la liste des cartes autorisées :

- Tous les traitements du terminal peuvent alors être
20 autorisés, notamment ceux concernant l'échange de messages avec la carte selon le protocole ISO 7816, la sélection des autres traitements validés dépendant des fonctionnalités souhaitées dans le cadre de cette adaptation.

Le comportement précité est alors appliqué par le terminal
25 équipement interlocuteur A si ce dernier a authentifié la carte à l'étape de test 2 et si l'identifiant de la carte $IdB = UA$ est contenu dans la liste connue par le terminal des cartes considérées comme inscrites dans la liste des cartes autorisées en raison des comportements qui leur sont associés.

Dans ces conditions, et sur réponse positive à l'étape de test 2
30 relative à l'équipement interlocuteur A de la figure 2a, le comportement est lu sous forme d'une chaîne de bits à la valeur zéro ou un successivement, chaîne de bits identifiée par RCA_k représentative du comportement choisi.

- Comportement vis-à-vis d'une carte préchargée non rechargeable :
 - Dans cette situation, on comprend que la carte, jouant le rôle d'équipement interlocuteur réciproque B, cette dernière comporte des droits pré-inscrits, ces droits pré-inscrits ne pouvant pas être renouvelés.

5

Dans ces conditions, le comportement du terminal de désembrouillage, équipement interlocuteur A, peut correspondre à une invalidation des traitements concernant l'échange avec la carte de messages relatifs à la gestion des titres d'accès inscrits sur la carte, c'est-à-dire à l'invalidation de messages de type EMM, messages de gestion par exemple. La sélection des autres traitements validés, pour le terminal de désembrouillage équipement interlocuteur A, dépend des fonctionnalités souhaitées vis-à-vis de ce type de carte. En particulier, et pour assurer l'utilisation de la carte par l'utilisateur qui a acquis cette carte pendant la durée autorisée par les droits pré-inscrits, l'envoi des messages de contrôle d'accès, dits messages ECM à la carte, est, bien entendu, valide.

15

Ce comportement est appliqué par le terminal équipement interlocuteur A si celui-ci a authentifié la carte équipement interlocuteur réciproque B et si le type de carte correspond à une carte préchargée non rechargeable.

20

- Comportement par défaut :
 - Ce comportement par défaut correspond à l'étape 3 de la figure 2a relativement à l'équipement interlocuteur A.

25

Un tel comportement est appliqué par le terminal vis-à-vis de la carte si ce dernier a authentifié la carte, et si, en réponse au test d'appartenance de l'étape 2, l'identifiant de la carte IdB n'appartient pas à la liste L_IDA du terminal. Dans ces conditions, aucun comportement spécifique ne peut être sélectionné pour le terminal, équipement interlocuteur A, vis-à-vis de la carte, équipement interlocuteur réciproque B. Dans ces conditions, le comportement par défaut peut être, à titre d'exemple non limitatif :

30

- tous les traitements du terminal sont autorisés, notamment ceux concernant l'échange de messages avec la carte.

Enfin, et dans le cadre de la mise en œuvre du protocole objet de la présente invention, on indique que, dans un mode de réalisation spécifique
5 ~~préférentiel non limitatif, les étapes consistant à inscrire, dans chaque~~
équipement interlocuteur ou chaque équipement interlocuteur réciproque, les liste d'identifiants d'équipements, liste d'identifiants de comportements et liste d'associations entre un identifiant d'équipements et un identifiant de
10 comportements sont, de manière préférentielle, mises en œuvre par transmission de messages de gestion de droits d'accès, messages EMM, ainsi que mentionné précédemment dans la description. On comprend, en particulier, que les procédures d'inscription précitées peuvent concerner soit la première inscription des listes précitées dans des équipements existants, soit, au
15 contraire, la mise à jour de listes existantes telles que décrites précédemment.

Des exemples spécifiques de comportements plus particulièrement adaptés à la gestion d'un terminal de désembrouillage, jouant par exemple le rôle d'équipement interlocuteur A, et d'une carte dédiée, allouée à un utilisateur habilité, jouant le rôle d'équipement interlocuteur réciproque B, lorsque la
20 procédure d'authentification entre le terminal de désembrouillage et la carte est une procédure à plus d'un niveau d'authentification, seront maintenant donnés ci-après.

Le processus, ou mode opératoire, du protocole objet de la présente invention dans le cas précité, est strictement conforme au protocole décrit en
25 liaison avec la figure 2b, la procédure d'authentification comportant un niveau d'authentification forte, un niveau d'authentification intermédiaire et un niveau d'authentification nulle, ainsi que décrit précédemment en liaison avec la figure précitée.

Dans ces conditions, le protocole objet de l'invention peut consister, suivant le niveau d'authentification réussie et en fonction de l'identité de
30 l'équipement interlocuteur réciproque par exemple :

- pour un niveau d'authentification forte réussie, c'est-à-dire sur réponse positive à la sous-étape 4₁ de la figure 2b, à autoriser un mode d'accès

par achat impulsif à la sous-étape 4₂ précédemment décrite en liaison avec la figure 2b. On rappelle que le mode d'accès par achat impulsif fait l'objet d'une définition dans la norme UTE C 90 007.

- au contraire, pour un niveau d'authentification intermédiaire réussie, c'est-à-dire un niveau d'authentification correspondant à un niveau d'authentification forte non réussie, soit sur réponse négative à la sous-étape de test 4₁ précitée, mais, suite à une présentation d'un code porteur de carte équipement interlocuteur réciproque réussie, suite à la mise en œuvre des étapes 0₂, 6₁ et 6₂ de la figure 2b, le protocole objet de l'invention peut consister alors à autoriser le traitement de tous les messages de gestion, messages EMM, et de tous les messages de contrôle d'accès, messages ECM, précédemment mentionnés dans la description en dehors du mode d'accès par achat impulsif.

On comprend, en particulier, que, pour autoriser l'achat impulsif, cette autorisation soit rendue consécutive à la vérification d'un niveau d'authentification forte afin, par exemple, d'assurer la sécurité des transactions relatives aux achats impulsifs.

- au contraire, pour un niveau d'authentification nulle seule réussie, c'est-à-dire sur réponse négative non seulement à la sous-étape 4₁ précitée, mais également à la sous-étape 6₂ précédemment mentionnée dans la description, le niveau d'authentification nulle correspond alors à un niveau d'authentification forte non réussie et à une présentation d'un code porteur d'équipement interlocuteur réciproque, c'est-à-dire de carte, non réussie. Le protocole objet de l'invention consiste alors à autoriser le traitement des seuls messages de gestion, messages EMM précédemment cités dans la description. On comprend, dans ce dernier cas, que l'autorisation de traitement des seuls messages de gestion EMM permet de contrôler les actions effectuées par l'utilisateur de la carte, c'est-à-dire de l'équipement interlocuteur réciproque B, ce dernier pouvant alors uniquement procéder à des opérations de mise à jour des droits inscrits dans la carte, c'est-à-dire dans l'équipement interlocuteur réciproque, de valeurs cryptographiques ou autres, afin de permettre une mise à jour totale de l'ensemble des données inscrites dans l'équipement interlocuteur réciproque et permettre ensuite à ce dernier de mettre en œuvre le

protocole objet de la présente invention selon toutes les possibilités représentées en figure 2b.

Des exemples de mise en œuvre du protocole objet de la présente invention, permettant l'adaptation de l'interactivité entre plusieurs équipements informatiques d'un ensemble donné d'équipements informatiques, seront
5 maintenant donnés en liaison avec les figures 3a, 3b et les figures suivantes.

La figure 3a concerne l'application du protocole objet de la présente invention à un ensemble de N équipements connectés en réseau par exemple et susceptibles chacun d'exécuter un dialogue interactif avec un autre
10 équipement de cet ensemble d'équipements.

Sur la figure 3a, le nombre d'équipements est volontairement limité à cinq afin de ne pas surcharger le dessin.

Dans une telle situation, le protocole objet de la présente invention consiste à attribuer à un équipement, l'équipement A par exemple, la qualité
15 d'équipement interlocuteur pour toute transaction par transmission d'un message de requête vers un autre équipement de cet ensemble d'équipements.

A titre d'exemple non limitatif, sur la figure 3a, l'équipement A est équipement interlocuteur ei_1 , pour une première transaction vis-à-vis de l'équipement D, lequel est alors équipement interlocuteur réciproque eir_1 , pour
20 la même transaction 1.

Le protocole objet de l'invention consiste également à attribuer, à cet autre équipement, l'équipement D et, pour cette transaction, la transaction 1, la qualité d'équipement interlocuteur réciproque.

Il consiste également à attribuer, à l'équipement interlocuteur A, la
25 qualité d'interlocuteur réciproque, pour toute autre transaction distincte de cette transaction, la transaction 1, sur réception par cet équipement, l'équipement interlocuteur A, d'un message de requête provenant d'un autre équipement distinct appartenant à l'ensemble des équipements précités.

Sur la figure 3a, on comprend que l'équipement interlocuteur A
30 devient équipement interlocuteur réciproque eir_4 vis-à-vis de la transaction 4 initiée par l'équipement E, équipement interlocuteur pour la transaction 4 précitée. L'équipement E constitue l'autre équipement distinct de l'équipement A

auquel, pour la transaction 4, la qualité d'équipement interlocuteur ei_4 a été attribuée.

Le protocole objet de la présente invention consiste ainsi à appliquer, successivement, ce protocole entre tout équipement, tout autre équipement et
5 tout autre équipement distinct appartenant à l'ensemble d'équipements auxquels la qualité d'équipement interlocuteur et/ou la qualité d'équipement interlocuteur réciproque a été attribuée successivement.

Ainsi, le protocole objet de la présente invention permet d'exécuter un dialogue interactif adapté entre tous les équipements de cet ensemble
10 d'équipements par couples d'équipements auxquels la qualité d'interlocuteur respectivement d'interlocuteur réciproque a été attribuée. On comprend, en particulier, que la succession des transactions et le numéro d'ordre attribué à ces dernières ne sont pas représentatifs de la succession temporelle de celles-ci. Un tableau relatif à la figure 3a est introduit, ci-après, dans lequel les états
15 successifs d'équipement interlocuteur respectivement d'équipement interlocuteur réciproque sont indiqués pour les équipements A, B, C, D, E et les transactions 1, 2, 3, 4 représentés sur la figure 3a.

20

Tableau (Figure 3a)

t \ EQ	A	B	C	D	E
1	ei_1			eir_1	
2			eir_2	ei_2	
3		eir_3	ei_3		
4	eir_4				ei_4

Un autre exemple de mise en œuvre du protocole objet de la
25 présente invention, dans le cas de l'utilisation d'un terminal et d'une pluralité de cartes destinées à conduire un dialogue interactif avec ce terminal sera maintenant donné en liaison avec la figure 3b.

Dans cette situation, on considère un tel terminal de désembrouillage par exemple ou un terminal lecteur de carte bancaire par exemple, lequel est destiné à exécuter un dialogue interactif avec plusieurs de ces cartes, successivement.

5 A titre d'exemple non limitatif, sur la figure 3b, on a représenté un terminal, formé par un équipement informatique A constituant un équipement interlocuteur par exemple, et une pluralité de cartes B, C, D, E destinées à entrer en communication successivement avec le terminal A. On comprend, en particulier, que les cartes peuvent être introduites successivement dans le
10 lecteur de cartes du terminal A ou, au contraire, que chaque carte peut être couplée à un lecteur de carte et à un système auxiliaire non représenté au dessin, le système auxiliaire muni de la carte étant en mesure d'entrer en communication successivement avec le terminal A par exemple.

Selon un aspect du protocole objet de la présente invention, au
15 terminal A est attribué, par exemple, le rôle d'équipement interlocuteur pour chaque transaction successivement.

Dans ces conditions, l'équipement A est équipement interlocuteur ei_1 , ei_2 , ei_3 , ei_4 successivement pour chacune des transactions.

Au contraire, chaque équipement B, C, D, E est alors, en
20 conséquence, équipement interlocuteur réciproque pour la transaction correspondante, transactions 3, 4, 1, 2, ainsi que représenté sur la figure 3b. Le tableau relatif à la figure 3b résume l'état successif de chacun des équipements représentés sur la figure précitée.

25 Tableau (Figure 3b)

$t \backslash EQ$	A	B	C	D	E
1	ei_1			eir_1	
2	ei_2				eir_2
3	ei_3	eir_3			
4	ei_4		eir_4		

Une description plus détaillée de différentes variantes de mise en œuvre du protocole objet de la présente invention pour un ensemble N déterminé d'équipements connectés en réseau par exemple et susceptibles chacun d'exécuter un dialogue interactif avec un autre équipement de cet ensemble d'équipements, sera maintenant donnée successivement en liaison avec les figures 4a à 4f et 5a.

En référence à la figure 4a, on indique que le nombre N d'équipements n'est pas limité, mais que, afin de ne pas surcharger les dessins, le nombre d'équipements représentés sur les figures 4a et 5 par exemple est réduit à trois de manière non limitative.

En référence à la figure 4a, on indique que le protocole objet de la présente invention consiste à attribuer à l'un des équipements, l'équipement A par exemple, la qualité d'équipement interlocuteur pour toute transaction par transmission d'un message de requête vers une pluralité d'autres équipements sous-ensemble de l'ensemble d'équipements précité. Sur la figure 4a, le sous-ensemble d'équipements est représenté par l'équipement B et l'équipement C.

A titre d'exemple non limitatif, on rappelle que l'équipement A jouant le rôle d'équipement interlocuteur, dispose de la liste d'identifiants d'équipements L_ID_A , de la liste d'identifiants de comportements L_C_A comportant les différents identifiants de comportements RCA_k et de la liste d'associations L_IC_A entre un identifiant d'équipements et un identifiant de comportements. Les listes précitées correspondent, par exemple, aux listes déjà définies en relation avec la figure 1 ou la figure 2a.

Il en est de même en ce qui concerne l'équipement B, lequel dispose de la liste d'identifiants d'équipements L_ID_B , de la liste d'identifiants de comportements L_C_B , des identifiants de comportements RCB_h et de la liste d'associations L_IC_B . Ces listes correspondent également aux listes dont dispose l'équipement B dans la figure 2a par exemple.

De la même manière, et à titre d'exemple non limitatif, l'équipement C dispose :

- d'une liste d'identifiants d'équipements vérifiant la relation :
 - $L_ID_C = [IdA, IdB, \dots, IdF]$,
- d'une liste d'identifiants de comportements vérifiant la relation :

- $L_{C_c} = [RCC_1, RCC_2, \dots, RCC_l, \dots, RCC_s]$, les identifiants de comportements RCC_l vérifiant la relation :

- $RCC_l = [CC_1, CC_2, \dots, CC_o]$, les éléments CC_1 à CC_o définissant des références de comportement ou comportement élémentaire par exemple ;

5 - d'une liste d'associations entre un identifiant d'équipements et un identifiant de comportements vérifiant la relation :

- $L_{IC_c} = [[IdA[RCC_1]]; [IdB[RCC_l]]; \dots]$.

L'ensemble des listes précitées est représenté en figure 4b.

10 En référence à la figure 4a, on indique que le protocole objet de la présente invention consiste à attribuer, à chacun des autres équipements destinataires du message de requête, c'est-à-dire aux équipements B et C, pour la transaction précitée, la qualité d'équipement interlocuteur réciproque vis-à-vis de l'équipement interlocuteur A.

15 Il consiste ensuite à appliquer le protocole entre l'équipement auquel la qualité d'équipement interlocuteur a été attribuée, c'est-à-dire l'équipement A, et chacun des autres équipements, équipement B et équipement C du sous-ensemble d'équipements.

20 Dans ces conditions, conformément au protocole objet de l'invention, celui-ci comporte, au niveau de l'équipement interlocuteur A, une procédure d'authentification entre l'équipement interlocuteur et chacun des autres équipements de la pluralité d'équipements auxquels la qualité d'équipement interlocuteur réciproque a été attribuée, c'est-à-dire aux équipements B et C. Cette procédure d'authentification est mise en œuvre à partir de l'étape 1 représentée sur la figure 4a vis-à-vis de l'équipement B respectivement de 25 l'équipement C, ces étapes étant conformes au mode de mise en œuvre tel que représenté en figure 1 ou 2a par exemple.

30 Suite à la procédure d'authentification, une procédure de discrimination du comportement de l'équipement interlocuteur A vis-à-vis de chacun des autres équipements de la pluralité d'autres équipements, équipement B et C, auxquels la qualité d'équipement interlocuteur réciproque a été attribuée, est appelée.

La procédure de discrimination comprend une étape de test 2 comparable à celle mise en œuvre dans le cadre de la figure 2a, permettant de

vérifier l'appartenance de l'identifiant IdB respectivement IdC à la liste des identifiants L_{IDA} de l'équipement interlocuteur A. Sur réponse négative au test 2 précité pour chacun des autres équipements B et C, le comportement par défaut 3 est appelé. Au contraire, sur réponse positive au test 2 d'appartenance
 5 des identifiants à la liste des identifiants d'équipements précitée, l'étape 4 de récupération du comportement de l'équipement interlocuteur A associé à l'identifiant IdB , IdC est appelée de manière semblable au mode opératoire de la figure 2a par exemple. De même que dans le cas de la figure précitée, le comportement est associé à chaque identifiant d'équipements et au résultat de
 10 la procédure d'authentification.

Les étapes 4 de récupération du comportement précitées peuvent alors être suivies d'une procédure 5 de détermination du comportement commun de l'équipement interlocuteur A vis-à-vis de chacun des autres équipements B et C, auxquels la qualité d'équipement interlocuteur réciproque
 15 a été attribuée.

Cette opération de calcul du comportement commun CC_{ABC} correspond à une opération logique sur les comportements associés à chacun des équipements interlocuteurs réciproques B et C. Elle est représentée à l'étape 5 de la figure 4a et est notée $CC_{ABC} = RCA_x \otimes RCA_y$.

20 On comprend, en effet, que, pour un comportement de l'équipement interlocuteur A vis-à-vis de chacun des autres équipements interlocuteurs réciproques B respectivement C constitué par un identifiant de comportements désignant une liste de comportements élémentaires de cet équipement interlocuteur, la procédure de détermination du comportement commun
 25 consiste à calculer, par l'opération logique précitée, sur les listes précédemment mentionnées, la liste de comportements élémentaires résultant de l'opération logique réalisée sur les listes définissant ces comportements.

Ainsi, dans la relation précédente, CC_{ABC} désigne le comportement commun de A vis-à-vis de B et C et RCA_x et RCA_y désignent les identifiants de
 30 comportements du terminal interlocuteur A vis-à-vis de l'équipement interlocuteur réciproque B respectivement de l'équipement interlocuteur réciproque C.

Dans un premier mode de réalisation tel que représenté en figure 4c, l'étape 5 peut consister, pour le calcul du comportement commun précité, à partir de la liste d'associations L_{ICA} et, en particulier, vis-à-vis des éléments de listes dont la tête correspond aux identifiants IdB , respectivement IdC , à déterminer les comportements correspondants RCA_1 , RCA_p , le comportement commun étant déterminé par le calcul de l'intersection des listes représentatives des comportements identifiés par RCA_1 et RCA_p par exemple, selon la relation :

$$CC_{ABC} = RCA_1 \cap RCA_p.$$

En fait, il est possible de calculer l'intersection des listes de tous les comportements affectés à chacun des équipements interlocuteurs réciproques, et donc aux identifiants IdB et IdC , et de retenir la liste résultante la plus favorable.

Alors que le mode opératoire de la figure 4c est plus particulièrement réservé à des terminaux, c'est-à-dire à des équipements connectés en réseau, dans le cas où le protocole objet de la présente invention est mis en œuvre à partir d'un terminal de désembrouillage constituant par exemple équipement interlocuteur A et où une pluralité de cartes dédiées allouées aux abonnés est associée à un tel terminal de désembrouillage, le protocole objet de la présente invention peut également être mis en œuvre, ainsi que représenté en figure 4d.

Dans cette situation, seule la nature de la liste d'associations L_{ICA} est modifiée dans la mesure où les identifiants de comportements sont constitués non plus par des listes, mais par des chaînes de bits de valeur spécifique, les chaînes b et c par exemple, tel que représenté sur la figure 4d précitée.

Ainsi, on considère à nouveau chaque chaîne de bits comme un élément de liste ou une structure de données équivalente.

L'opération logique sur les comportements identifiés par les identifiants de comportements, tels que les comportements b et c par exemple, peut alors être mise en œuvre de manière semblable à celle représentée en figure 4c.

Dans ces conditions, le comportement commun CC_{ABC} vérifie la relation :

$$CC_{ABC} = b \cap c = \text{bitand}(b, c).$$

Dans la relation précédente, on indique que la fonction bitand désigne l'opération d'intersection, c'est-à-dire l'opération logique ET bit à bit entre les éléments b et c par exemple.

5 Bien entendu, l'opération logique sur les comportements représentés par des listes n'est pas limitée à l'opération d'intersection de listes.

A titre d'exemple non limitatif, on indique que la procédure de détermination du comportement commun peut consister à calculer la liste résultant de l'union des listes de comportements.

10 Ainsi que représenté en figure 4e, pour des terminaux connectés en réseau par exemple, l'étape 5 représentée en figure 4a peut consister en l'appel de la liste L_{ICA} , liste d'associations entre un identifiant d'équipements et un identifiant de comportements de l'équipement interlocuteur A et en un calcul de l'union des listes de comportements élémentaires identifiées par RCA_1 et RCA_p par exemple pour définir le comportement commun CC_{ABC} vérifiant la relation :

$$CC_{ABC} = RCA_1 \cup RCA_p.$$

En ce qui concerne la mise en œuvre du protocole objet de l'invention, dans le cadre d'un terminal, tel qu'un terminal de désembrouillage et d'une pluralité de cartes associées à ce dernier, l'opération sur les 20 comportements désignés par b et c sur la figure 4f, ces comportements étant définis par des chaînes de bits, peut correspondre à une opération d'union, le comportement commun étant alors défini par la relation :

$$CC_{ABC} = b \cup c = \text{bitor}(b, c).$$

On indique que la relation bitor représente l'opération OU(OR) bit à 25 bit entre les éléments b et c. Le résultat de l'opération, dans l'exemple donné en figure 4f, est égal à 010011.

Un autre exemple de mise en œuvre du protocole objet de la présente invention, pour un ensemble donné de N équipements connectés en réseau par exemple, chaque équipement étant susceptible d'exécuter un 30 dialogue interactif avec un autre équipement de cet ensemble, sera maintenant décrit en liaison avec la figure 5.

De même que dans le cas de la figure 4a, on indique que le nombre d'équipements N constitutif de l'ensemble des équipements n'est pas limité,

mais que, pour ne pas surcharger le dessin, le nombre d'autres équipements distincts de l'équipement A, considéré comme équipement interlocuteur, est limité à deux, les équipements B et C.

De même que dans le cas de la figure 4a, on indique que chaque
 5 équipement, équipement interlocuteur A et équipements interlocuteurs
 réciproques B et C, dispose de liste d'identifiants d'équipements L_ID_A, L_ID_B et
 L_ID_C, de liste d'identifiants de comportements L_C_A, L_C_B et L_C_C, de liste
 d'associations entre un identifiant d'équipements et un identifiant de
 comportements L_IC_A, L_IC_B et L_IC_C, telles que définies précédemment en
 10 relation avec la figure 4a précitée. A titre d'exemple, les listes précitées peuvent
 correspondre à celles représentées en figure 4b.

En particulier, on indique que le comportement élémentaire identifié
 par l'identifiant de comportements auquel est associé un identifiant
 d'équipements peut lui-même être constitué par une liste de comportements
 15 élémentaires ou de références de comportements, lesquels peuvent être des
 comportements indépendants des fonctionnalités de chaque équipement
 informatique A, B ou C.

En référence à la figure 5, on indique que le protocole objet de
 l'invention consiste alors à attribuer à un équipement, l'équipement A par
 20 exemple, la qualité d'équipement interlocuteur pour toute transaction par
 transmission d'un message de requête vers une pluralité d'autres équipements,
 les équipements B et C limités à deux, comme dans le cas de la figure 4a.

Le protocole objet de l'invention consiste en outre à attribuer, à
 l'ensemble constitué des autres équipements destinataires, les équipements B
 25 et C précités, de ce message de requête, pour la transaction considérée, la
 qualité d'équipement interlocuteur réciproque vis-à-vis de l'équipement
 interlocuteur A.

Il consiste ensuite à appliquer le protocole selon l'invention entre
 l'équipement A, auquel la qualité d'équipement interlocuteur a été attribuée, et
 30 l'ensemble constitué des autres équipements formant le sous-ensemble
 d'équipements auxquels la qualité d'équipement interlocuteur réciproque a été
 attribuée, le protocole comportant, au niveau de l'équipement interlocuteur, une

procédure 1 d'authentification de chacun des autres équipements auxquels la qualité d'équipement interlocuteur réciproque B et C a été attribuée.

Sur la figure 5, on indique que la procédure d'authentification correspond à l'étape 1 de la figure 4a par exemple, au cours de laquelle la
 5 récupération des identifiants IdB respectivement IdC est effectuée, puis la vérification des valeurs d'authentification selon les opérations $\mathcal{V}(\text{Auth}(\text{IdB}))$ et $\mathcal{V}(\text{Auth}(\text{IdC}))$ est réalisée. La procédure d'authentification peut correspondre à celle décrite en liaison avec les figures 1, 2a ou 4a précédentes.

En fonction du résultat de la procédure d'authentification 1 précitée,
 10 réalisée pour chacun des équipements interlocuteurs réciproques et des niveaux d'authentification vérifiés, chaque équipement interlocuteur réciproque est considéré comme susceptible, individuellement, d'exécuter un dialogue interactif avec l'équipement interlocuteur A.

Selon un aspect remarquable du mode de mise en œuvre spécifique
 15 du protocole objet de la présente invention, tel que représenté en figure 5, celui-ci consiste ensuite à appeler une procédure 1₁ d'authentification conjointe du sous-ensemble des équipements interlocuteurs réciproques vis-à-vis de l'équipement interlocuteur A.

En fonction du résultat de cette procédure d'authentification conjointe,
 20 le sous-ensemble des équipements interlocuteurs réciproques B et C est authentifié en qualité d'équipement interlocuteur réciproque conjoint pour l'exécution de la transaction vis-à-vis de l'équipement interlocuteur A.

Sur la figure 5, l'opération de procédure d'authentification conjointe est représentée sous la forme de l'étape 1₁ permettant d'effectuer le calcul de
 25 la valeur logique d'authentification conjointe vérifiant la relation :

$$- \mathcal{V}_{cc} = \mathcal{V}(\text{Auth}(\text{IdB})) \text{ ET } \mathcal{V}(\text{Auth}(\text{IdC}))$$

La procédure d'authentification conjointe 1₁ peut alors être suivie d'une procédure 2 d'habilitation conjointe du sous-ensemble des équipements interlocuteurs réciproques, à l'exécution du dialogue interactif vis-à-vis de
 30 l'équipement interlocuteur A.

Ainsi que représenté sur la figure 5, la procédure d'habilitation conjointe peut consister à vérifier l'appartenance de l'identifiant de l'ensemble

constitué des équipements A et B, interlocuteur réciproque, cet ensemble étant limité à deux dans le cadre non limitatif de la figure 5, à la liste d'identifiants d'équipements L_{IDA} de l'équipement interlocuteur A.

Sur réponse négative au test d'habilitation conjointe 2, la procédure d'application du comportement par défaut 3 peut être appelée, cette procédure pouvant, par exemple, correspondre à la procédure de comportement par défaut 3 précédemment décrite dans la description en liaison avec la figure 4a. Le comportement par défaut est, dans ce cas, défini en fonction du résultat de la procédure d'authentification conjointe \mathcal{O}_{cc} .

Au contraire, sur réponse positive au test d'habilitation conjointe, une procédure 4 de discrimination ou de récupération du comportement conjoint de l'équipement interlocuteur A vis-à-vis du sous-ensemble des équipements interlocuteurs réciproques B, C, sous-ensemble auquel la qualité d'interlocuteur réciproque conjoint a été attribuée, est appelée, cette procédure de discrimination correspondant sensiblement à une procédure de récupération du comportement conjoint, tel qu'il sera décrit ultérieurement dans la description.

L'étape 4 de discrimination du comportement conjoint est alors suivie d'une procédure 5 d'application du comportement conjoint de l'équipement interlocuteur vis-à-vis des autres équipements formant le sous-ensemble auquel la qualité d'interlocuteur réciproque conjoint a été attribuée.

Le protocole objet de la présente invention permet d'appliquer un comportement conjoint de tout équipement d'un ensemble d'équipements vis-à-vis de toute pluralité d'équipements formant un sous-ensemble de cet ensemble d'équipements, sous-ensemble auquel la qualité d'interlocuteur réciproque conjoint a été attribuée.

Un exemple de mise en œuvre spécifique sera décrit en liaison avec les figures 5 et 4b.

Sur la figure 4b, on a représenté des structures de liste permettant la mise en œuvre du protocole objet de la présente invention, tel que décrit précédemment dans la description en liaison avec la figure 5.

En référence à la figure 5, on indique que le test de l'étape 2 consiste à déterminer si l'identifiant composé, formé par les identifiants (IdB, IdC), est inclus dans la liste d'identifiants d'équipement L_{IDA} de l'équipement

interlocuteur A. L'identifiant composé (IdB, IdC) formé par l'identifiant des équipements interlocuteurs réciproques B et C représente un identifiant d'équipements interlocuteurs réciproques habilités à participer à la transaction et agréé comme identifiant d'équipements interlocuteurs réciproques conjoints
 5 vis-à-vis de l'équipement interlocuteur A.

En référence à la figure 5, on indique que la procédure de discrimination du comportement conjoint de l'équipement interlocuteur A vis-à-vis du sous-ensemble des équipements interlocuteurs réciproques B et C peut consister à sélectionner l'association entre l'identifiant composé et l'identifiant
 10 de comportements.

On comprend, en effet, qu'à partir de l'identifiant composé (IdB, IdC), on procède, à l'étape 4, à l'appel des comportements définis par exemple dans la liste d'associations L_{ICA} , c'est-à-dire des identifiants de comportements
 15 RCA_1, RCA_k , pour l'identifiant composé d'équipements (IdB, IdC) correspondant précédemment cité.

L'étape 4 est alors suivie d'une étape 5 consistant à appliquer le comportement conjoint.

En référence à la figure 5 et à la figure 4b, pour l'identifiant composé
 20 (IdB, IdC), le comportement conjoint peut être défini par une opération logique sur les identifiants de comportements RCA_1, RCA_k précités. Ce comportement est appliqué au sous-ensemble formé par les équipements interlocuteurs réciproques B et C.

On comprend bien sûr, qu'en fonction des valeurs codées de
 25 comportements élémentaires ou références de comportements CA_1, CA_2, \dots, CA_p constitutives de chaque identifiant de comportements, le produit logique précité correspond à un comportement conjoint en fonction de la logique appliquée au produit précité.

A titre d'exemple non limitatif, on indique que les comportements
 30 élémentaires ou références de comportements précités peuvent correspondre à des comportements fonctionnels très élaborés.

Ainsi, le comportement élémentaire CA_1 peut consister en une valeur codée, constitutive d'un élément commun détenu par l'ensemble des utilisateurs

des équipements interlocuteurs et interlocuteurs réciproques, cet élément commun consistant, par exemple, en un code ou un mot de passe autorisant chaque utilisateur, par l'intermédiaire de l'équipement dont il dispose, à prendre part à la transaction précitée. Les autres comportements successifs CA₂ à CA_p peuvent, par exemple, correspondre à des paramètres fonctionnels très divers, tels que utilisation d'une langue commune parmi plusieurs langues pour la transaction, utilisation de paramètres spécifiques de chiffrement/déchiffrement pour la transaction ou analogues.

La mise en œuvre du protocole objet de la présente invention, lors de la définition d'un comportement conjoint, permet une application à des situations les plus diverses, telles que téléconférences, transactions multipostes sécurisées ou analogues.

REVENDEICATIONS

1. Protocole d'adaptation du degré d'interactivité entre un équipement interlocuteur et un équipement interlocuteur réciproque d'un ensemble d'équipements interlocuteurs, lorsque cet équipement interlocuteur et cet
5 équipement interlocuteur réciproque sont soumis à un dialogue interactif,

caractérisé en ce qu'il consiste au moins :

a) à inscrire, dans ledit équipement interlocuteur, une liste d'identifiants d'équipements interlocuteurs réciproques ;

b) à inscrire, dans ledit équipement interlocuteur, une liste
10 d'identifiants de comportements, lesdits comportements étant pertinents dans le cadre dudit dialogue interactif ;

c) à inscrire, dans ledit équipement interlocuteur, au moins une association entre un identifiant d'équipements et un identifiant de comportements, et, lors de la mise en présence de cet équipement interlocuteur
15 et d'au moins un équipement interlocuteur réciproque en vue de l'exécution de ce dialogue interactif ;

d) à effectuer une procédure d'authentification entre ledit équipement interlocuteur et ledit équipement interlocuteur réciproque, et,

- à rechercher l'identifiant de l'équipement interlocuteur réciproque
20 authentifié dans ladite liste d'identifiants ;

- à lire ledit identifiant de comportements associé ;

- à appliquer, au niveau de l'équipement interlocuteur, un comportement vis-à-vis de l'équipement interlocuteur réciproque authentifié, ce comportement étant sélectionné en fonction du résultat de la procédure
25 d'authentification et associé à l'identifiant de comportements et à l'identifiant de l'équipement interlocuteur réciproque.

2. Protocole selon la revendication 1, caractérisé en ce que, sur réponse négative à l'étape de recherche de l'identifiant de l'équipement interlocuteur réciproque authentifié dans la liste d'identifiants, celui-ci consiste à
30 appeler et appliquer une procédure de comportement par défaut sélectionné en fonction du résultat de ladite procédure d'authentification.

3. Protocole selon l'une des revendications 1 ou 2, caractérisé en ce que ladite procédure d'authentification entre équipement interlocuteur et

équipement interlocuteur réciproque est une procédure à plus d'un niveau d'authentification.

4. Protocole selon l'une des revendications 1 à 3 pour l'adaptation réciproque de l'interactivité entre un équipement interlocuteur et un équipement interlocuteur réciproque d'un ensemble d'équipements interlocuteurs, lorsque
 5 ~~cet équipement interlocuteur et cet équipement interlocuteur réciproque sont~~
 soumis à un dialogue interactif, caractérisé en ce qu'il consiste :

a) à inscrire, dans chaque équipement interlocuteur respectivement dans chaque équipement interlocuteur réciproque, une liste d'identifiants
 10 d'équipements interlocuteurs réciproques respectivement d'équipements interlocuteurs ;

b) à inscrire, dans chaque équipement interlocuteur respectivement dans chaque équipement interlocuteur réciproque, une liste d'identifiants de comportements, lesdits comportements étant définis dans le cadre dudit
 15 dialogue interactif ;

c) à inscrire au moins une association entre un identifiant d'équipements et un identifiant de comportements dans chaque équipement interlocuteur et chaque équipement interlocuteur réciproque, chaque équipement interlocuteur respectivement chaque équipement interlocuteur
 20 réciproque disposant au moins d'une association entre un identifiant d'équipements interlocuteurs réciproques et un identifiant de comportements, respectivement entre un identifiant d'équipements interlocuteurs et un identifiant de comportements ; et, lors de la mise en présence d'un équipement interlocuteur et d'un équipement interlocuteur réciproque en vue de l'exécution
 25 de ce dialogue interactif,

d) à effectuer une procédure d'authentification réciproque entre ledit équipement interlocuteur et ledit équipement interlocuteur réciproque ; et,

e) à rechercher l'identifiant de l'équipement interlocuteur réciproque authentifié respectivement de l'équipement interlocuteur authentifié dans
 30 lesdites listes d'identifiants ;

f) à lire au moins ledit identifiant de comportements associé dans l'équipement interlocuteur respectivement dans l'équipement interlocuteur réciproque ;

g) à appliquer, de manière indépendante, au niveau de l'équipement interlocuteur authentifié respectivement de l'équipement interlocuteur réciproque authentifié, un comportement vis-à-vis de l'équipement interlocuteur réciproque authentifié respectivement de l'équipement interlocuteur authentifié, ce comportement étant sélectionné en fonction du résultat de la procédure d'authentification et associé à l'identifiant de comportements et à l'identifiant de l'équipement interlocuteur réciproque respectivement à l'identifiant de comportements et à l'identifiant de l'équipement interlocuteur.

5. Protocole selon l'une des revendications 1 à 4, caractérisé en ce que ledit équipement interlocuteur comprend au moins, mémorisés dans une mémoire non volatile :

- une liste d'identifiants d'équipements interlocuteurs réciproques dont l'un des éléments de liste désigne l'identifiant dudit équipement interlocuteur réciproque ;

- une liste d'identifiants de comportements dudit équipement interlocuteur vis-à-vis d'un équipement interlocuteur réciproque, ladite liste comportant au moins un élément constituant une référence de comportement d'acceptation de dialogue interactif, de refus de dialogue interactif ou d'acceptation conditionnelle de dialogue interactif ;

- une liste d'associations entre un identifiant d'équipements et un identifiant de comportements, ladite liste d'associations permettant la mise en correspondance d'un élément de la liste d'identifiants d'équipements interlocuteurs réciproques et d'un élément de la liste d'identifiants de comportements .

6. Protocole selon l'une des revendications 4 ou 5, caractérisé en ce que ledit équipement interlocuteur réciproque comprend au moins, mémorisés dans une mémoire non volatile :

- une liste d'identifiants d'équipements interlocuteurs dont l'un des éléments de liste désigne l'identifiant dudit équipement interlocuteur ;

- une liste d'identifiants de comportements dudit équipement interlocuteur réciproque vis-à-vis d'un équipement interlocuteur, ladite liste comportant au moins un élément constituant une référence de comportement

d'acceptation de dialogue interactif, de refus de dialogue interactif ou d'acceptation conditionnelle de dialogue interactif ;

- une liste d'associations entre un identifiant d'équipements et un identifiant de comportements, ladite liste d'associations permettant la mise en correspondance d'un élément de la liste d'identifiants d'équipements interlocuteurs et d'un élément de la liste d'identifiants de comportements.

7. Protocole selon l'une des revendications 1 à 6, caractérisé en ce que ledit équipement interlocuteur est constitué par un terminal, équipé d'un lecteur de carte à microprocesseur, ledit équipement interlocuteur réciproque étant constitué par une carte à microprocesseur.

8. Protocole selon la revendication 7, caractérisé en ce que ledit équipement interlocuteur étant constitué par un terminal de désembrouillage d'informations embrouillées, lesdites informations embrouillées étant transmises en mode point-multipoint à partir d'un centre d'émission, le contrôle d'accès à ces informations étant effectué à partir de messages de contrôle d'accès contenant le cryptogramme d'un mot de contrôle et des critères d'accès transmis périodiquement avec les informations embrouillées et ledit équipement interlocuteur réciproque étant constitué par une carte à microprocesseur dédiée, jouant le rôle de module de contrôle d'accès, comportant au moins un processeur de sécurité et une mémoire non volatile programmable sécurisée comportant des droits d'accès inscrits, la gestion desdits droits d'accès inscrits étant effectuée à partir de messages de gestion des droits d'accès transmis avec les informations embrouillées, ledit contrôle d'accès à ces informations étant effectué sur vérification de l'identité d'au moins un droit de contrôle d'accès inscrit dans la carte et d'un des critères d'accès et par déchiffrement dans ledit équipement interlocuteur réciproque du cryptogramme du mot de contrôle à partir d'une clé d'exploitation, pour restituer le mot de contrôle permettant le désembrouillage des informations embrouillées dans ledit équipement interlocuteur à partir de ce mot de contrôle restitué, dans ledit équipement interlocuteur,

- ledit au moins un élément constituant une référence de comportement d'acceptation de dialogue interactif est constitué par une liste de

comportements vis-à-vis d'équipements interlocuteurs réciproques habilités à engager ledit dialogue interactif ;

- ledit au moins un élément constituant une référence de comportement de refus de dialogue interactif est constitué par une liste de
5 comportements vis-à-vis d'équipements interlocuteurs réciproques habilités à engager ledit dialogue interactif, auxquels la faculté d'engager ledit dialogue interactif a été retirée.

9. Protocole selon la revendication 8, caractérisé en ce que, dans ledit équipement interlocuteur réciproque,

- 10 - ledit au moins un élément constituant une référence de comportement d'acceptation de dialogue interactif est constitué par une liste de comportements vis-à-vis d'équipements interlocuteurs habilités à engager ledit dialogue interactif ;

- ledit au moins un élément constituant une référence de
15 comportement de refus de dialogue interactif est constitué par une liste de comportements vis-à-vis d'équipements interlocuteurs habilités à engager ledit dialogue interactif, auxquels la faculté d'engager ledit dialogue interactif a été retirée.

- 20 10. Protocole selon l'une des revendications 5 à 9, caractérisé en ce que ledit au moins un élément constituant une référence d'acceptation conditionnelle de dialogue interactif est constitué par une liste dont l'un au moins des éléments est représentatif d'un comportement fonctionnel dudit équipement interlocuteur réciproque respectivement dudit équipement interlocuteur.

- 25 11. Protocole selon l'une des revendications 5 à 9, caractérisé en ce que ledit au moins un élément constituant une référence d'acceptation conditionnelle de dialogue interactif est constitué par une liste dont l'un au moins des éléments est représentatif d'un comportement personnel de l'utilisateur dudit équipement interlocuteur réciproque respectivement dudit
30 interlocuteur.

12. Protocole selon l'une des revendications 8 à 11, caractérisé en ce que les étapes d'inscription dans chaque équipement interlocuteur et/ou chaque

équipement interlocuteur réciproque sont mises en œuvre par transmission de messages de gestion de droits d'accès.

13. Protocole selon l'une des revendications 8 à 12, caractérisé en ce que, pour une procédure d'authentification entre un terminal de
 5 désembrouillage, jouant le rôle d'équipement interlocuteur, et une carte, jouant le rôle d'équipement interlocuteur réciproque, comportant un niveau d'authentification forte, un niveau d'authentification intermédiaire et un niveau d'authentification nulle, celui-ci consiste, suivant le niveau d'authentification réussie et en fonction de l'identité dudit terminal interlocuteur réciproque :

- 10 • pour un niveau d'authentification forte réussie, à autoriser un mode d'accès par achat impulsif ;
- pour un niveau d'authentification intermédiaire réussie, correspondant à un niveau d'authentification forte non réussie, mais à une présentation d'un code utilisateur de l'équipement interlocuteur réciproque
 15 réussie, à autoriser le traitement de tous les messages de gestion et de tous les messages de contrôle d'accès en dehors du mode d'accès par achat impulsif ;
 et
- pour un niveau d'authentification nulle, correspondant à un niveau d'authentification forte non réussie et à une présentation d'un code utilisateur de
 20 l'équipement interlocuteur réciproque non réussie, à autoriser le traitement des seuls messages de gestion.

14. Protocole selon l'une des revendications 1 à 6, caractérisé en ce que, pour un ensemble de N équipements connectés en réseau et susceptibles
 25 chacun d'exécuter un dialogue interactif avec un autre équipement de cet ensemble d'équipements, ledit protocole consiste :

- à attribuer, à un équipement, la qualité d'équipement interlocuteur pour toute transaction par transmission d'un message de requête vers un autre équipement dudit ensemble d'équipements ;
- à attribuer, à cet autre équipement, pour cette transaction, la qualité
 30 d'équipement interlocuteur réciproque ;
- à attribuer, audit équipement, la qualité d'interlocuteur réciproque pour toute autre transaction, distincte de cette transaction, sur réception, par

ledit équipement d'un message de requête provenant d'un autre équipement distinct dudit ensemble d'équipements ;

- à attribuer, audit autre équipement distinct, la qualité d'équipement interlocuteur pour ladite autre transaction ;

- 5 - à appliquer ledit protocole entre tout équipement, tout autre équipement et tout autre équipement distinct dudit ensemble d'équipements, auquel la qualité d'équipement interlocuteur et/ou la qualité d'équipement interlocuteur réciproque a été attribuée, ce qui permet d'exécuter un dialogue interactif adapté entre tous les équipements de cet ensemble d'équipements
10 par couples d'équipements, auxquels la qualité d'interlocuteur respectivement d'interlocuteur réciproque a été attribuée.

15 15. Protocole selon l'une des revendications 1 à 6, caractérisé en ce que, pour un ensemble de N équipements connectés en réseau et susceptibles chacun d'exécuter un dialogue interactif avec un autre équipement de cet ensemble d'équipements, ledit protocole consiste :

- à attribuer, à un équipement, la qualité d'équipement interlocuteur pour toute transaction par transmission d'un message de requête vers une pluralité d'autres équipements, sous-ensemble dudit ensemble d'équipements ;

20 - à attribuer, à chacun desdits autres équipements destinataires dudit message de requête, pour cette transaction, la qualité d'équipement interlocuteur réciproque, vis-à-vis dudit équipement interlocuteur ;

25 - à appliquer ledit protocole entre cet équipement, auquel la qualité d'équipement interlocuteur a été attribuée, et chacun des autres équipements de ce sous-ensemble dudit ensemble d'équipements, ledit protocole comportant, au niveau dudit équipement interlocuteur :

• une procédure d'authentification entre ledit équipement interlocuteur et chacun desdits autres équipements de cette pluralité d'autres équipements auxquels la qualité d'interlocuteur réciproque a été attribuée, et, en fonction du résultat de chaque procédure d'authentification,

30 • une procédure de discrimination du comportement dudit équipement interlocuteur vis-à-vis de chacun desdits autres équipements de

cette pluralité d'autres équipements auquel la qualité d'équipement interlocuteur réciproque a été attribuée, et

- une procédure de détermination du comportement commun dudit équipement interlocuteur vis-à-vis de chacun desdits autres équipements de cette pluralité d'autres équipements auquel la qualité d'équipement interlocuteur réciproque a été attribuée, ce qui permet d'appliquer ledit comportement commun de tout équipement de cet ensemble d'équipements vis-à-vis des autres équipements de cette pluralité d'autres équipements sous-ensemble dudit ensemble d'équipements.

10 16. Protocole selon la revendication 15, caractérisé en ce que, pour un comportement dudit équipement interlocuteur vis-à-vis de chacun desdits autres équipements interlocuteurs réciproques, constitué par une liste de comportements élémentaires de cet équipement interlocuteur, ladite procédure de détermination du comportement commun consiste à calculer la liste résultant
15 de l'intersection desdites listes de comportements élémentaires.

 17. Protocole selon la revendication 15, caractérisé en ce que, pour un comportement dudit équipement interlocuteur vis-à-vis de chacun desdits autres équipements interlocuteurs réciproques constitué par une liste de comportements élémentaires de cet équipement interlocuteur, ladite procédure
20 de détermination du comportement commun consiste à calculer la liste résultant de l'union desdites listes de comportements élémentaires.

 18. Protocole selon l'une des revendications 1 à 6, caractérisé en ce que, pour un ensemble de N équipements connectés en réseau et susceptibles chacun d'exécuter un dialogue interactif simultanément avec un autre équipement de
25 cet ensemble d'équipements, ledit protocole consiste :

- à attribuer à un équipement la qualité d'équipement interlocuteur pour toute transaction par transmission d'un message de requête vers une pluralité d'autres équipements sous-ensemble dudit ensemble d'équipements ;
- à attribuer à chacun desdits autres équipements destinataires dudit
30 message de requête, pour cette transaction, la qualité d'équipement interlocuteur réciproque vis-à-vis dudit équipement interlocuteur ;
- à appliquer ledit protocole entre cet équipement, auquel la qualité d'équipement interlocuteur a été attribuée, et chacun des autres équipements

de ce sous-ensemble dudit ensemble d'équipements, auxquels la qualité d'équipement interlocuteur réciproque a été attribuée, ledit protocole comportant, au niveau dudit équipement interlocuteur :

- 5 • une procédure d'authentification de chacun desdits autres équipements auxquels la qualité d'équipement interlocuteur réciproque a été attribuée, et, en fonction du résultat de cette procédure d'authentification, chacun desdits autres équipements auxquels la qualité d'équipement interlocuteur réciproque a été attribuée étant susceptible, individuellement, d'exécuter un dialogue interactif avec ledit équipement, auquel la qualité

10 d'équipement interlocuteur a été attribuée,
- une procédure d'authentification conjointe du sous-ensemble des équipements interlocuteurs réciproques vis-à-vis dudit équipement interlocuteur, et, en fonction du résultat de cette procédure d'authentification conjointe, le sous-ensemble desdits équipements

15 interlocuteurs réciproques étant authentifié en qualité d'interlocuteur réciproque conjoint pour l'exécution de ladite transaction ;
- une procédure d'habilitation conjointe du sous-ensemble des équipements interlocuteurs réciproques à l'exécution du dialogue interactif vis-à-vis dudit équipement interlocuteur, et sur procédure d'habilitation conjointe

20 réussie,
- une procédure de discrimination du comportement conjoint dudit équipement interlocuteur vis-à-vis du sous-ensemble des équipements interlocuteurs réciproques auquel la qualité d'interlocuteur réciproque conjoint a été attribuée, et sur procédure de discrimination réussie,

25
- une procédure de détermination et d'application du comportement conjoint dudit équipement interlocuteur vis-à-vis desdits autres équipements auxquels la qualité d'interlocuteur réciproque conjoint a été attribuée, ce qui permet d'appliquer ledit comportement conjoint de tout équipement de cet ensemble d'équipements vis-à-vis de toute pluralité

30 d'équipements auquel la qualité d'interlocuteur réciproque conjoint a été attribuée.

19. Protocole selon la revendication 18, caractérisé en ce que ladite procédure d'authentification conjointe consiste à vérifier à la valeur vraie le produit logique des valeurs logiques représentatives de chaque procédure d'authentification réciproque.

5 20. Protocole selon l'une des revendications 18 ou 19, caractérisé en ce que ladite procédure d'habilitation conjointe consiste :

- à établir, à partir de ladite liste d'identifiants d'équipements interlocuteurs réciproques, inscrite dans ledit équipement interlocuteur, un identifiant composé formé par l'identifiant des équipements interlocuteurs réciproques habilités à
10 participer à ladite transaction et agréés comme identifiants d'équipements interlocuteurs réciproques pour lesquels la procédure d'authentification conjointe a été vérifiée à la valeur vraie, vis-à-vis de l'équipement interlocuteur.

21. Protocole selon la revendication 20, caractérisé en ce que ladite procédure de discrimination du comportement conjoint dudit équipement
15 interlocuteur vis-à-vis du sous-ensemble des équipements interlocuteurs réciproques consiste :

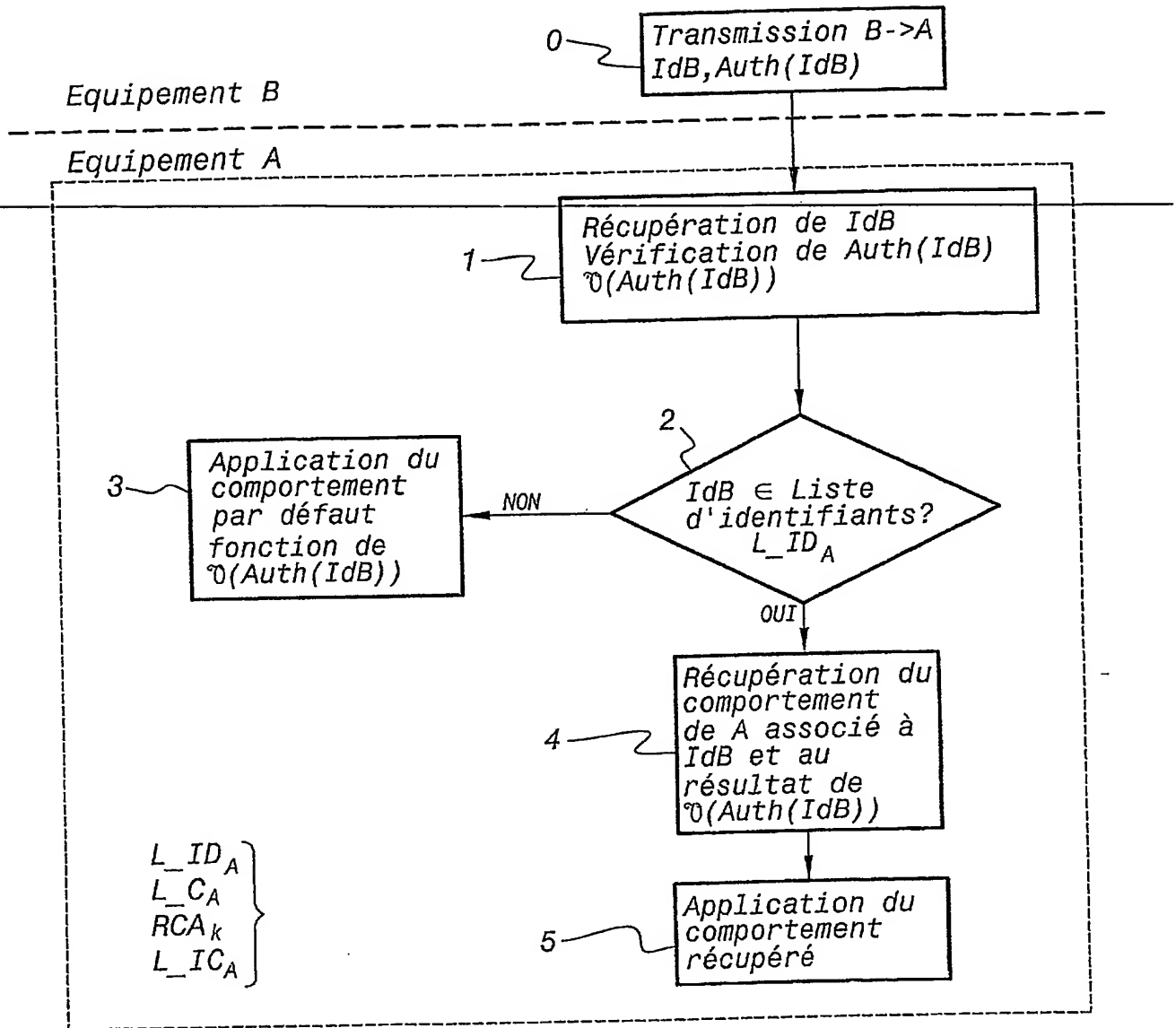
- à sélectionner l'association entre l'identifiant composé et un identifiant de comportements dans ledit équipement interlocuteur ;
- à procéder, à partir de l'identifiant composé, à l'appel des
20 comportements définis dans la liste d'associations.

22. Equipement informatique comprenant des moyens d'entrée/sortie permettant d'assurer la transmission et/ou la réception de messages dans le cadre d'un dialogue interactif avec un autre équipement informatique, des moyens de calcul reliés auxdits moyens d'entrée/sortie, une mémoire vive de
25 travail et au moins une mémoire non volatile programmable, caractérisé en ce que celui-ci comporte au moins, inscrits en mémoire non volatile :

- une liste d'identifiants d'équipements informatiques, accessibles par l'intermédiaire desdits moyens d'entrée/sortie ;
- une liste d'identifiants de comportements définis dans le cadre dudit
30 dialogue interactif ;
- au moins une liste d'associations entre un identifiant d'équipements et un identifiant de comportements.

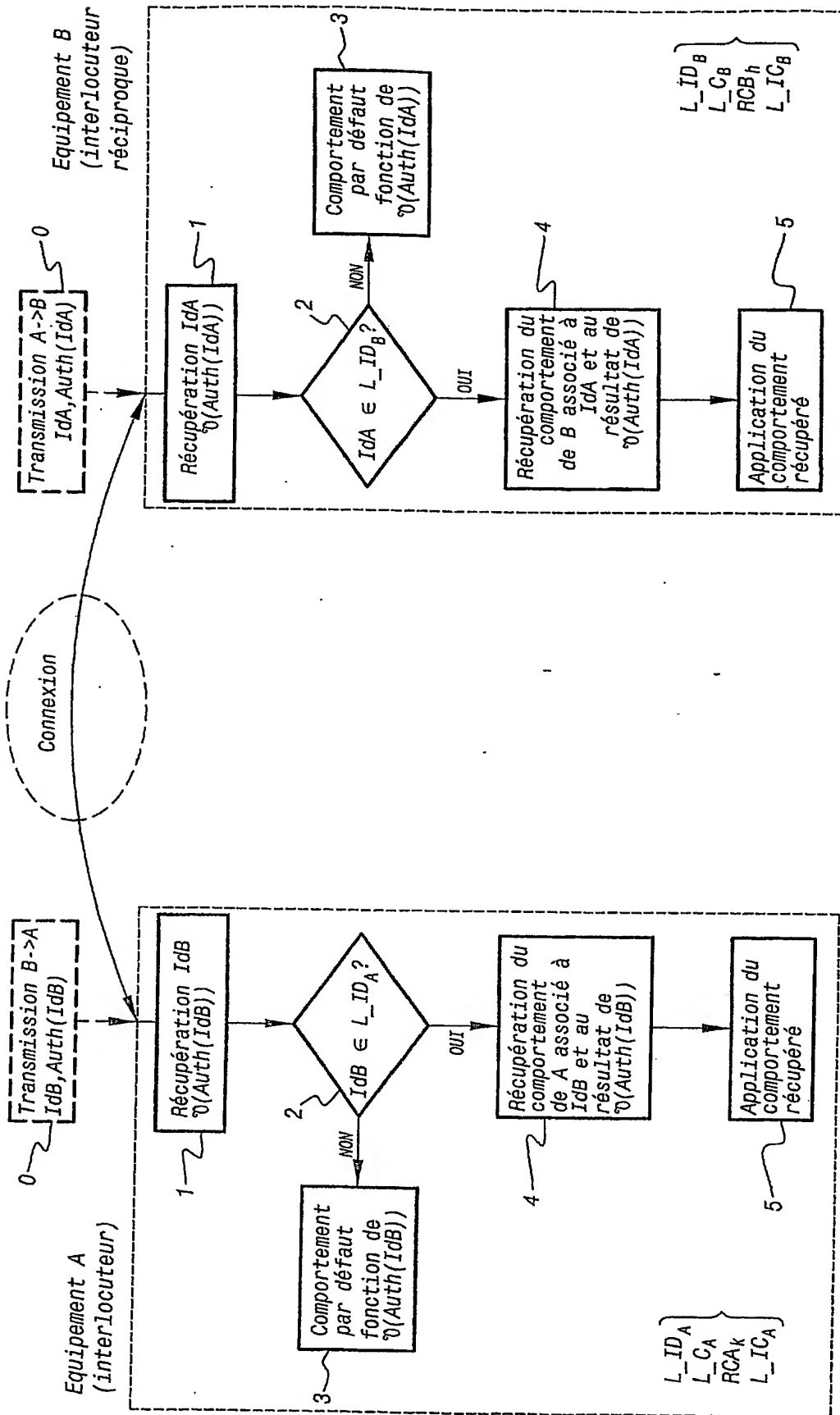
23. Equipement informatique selon la revendication 22, caractérisé en ce que celui-ci comporte, en outre, un processeur de sécurité et des moyens d'authentification de tout équipement informatique candidat à l'exécution d'un dialogue interactif avec ledit équipement informatique.

- 5 24. Equipement informatique selon l'une des revendications 22 ou 23, caractérisé en ce que celui-ci comporte des moyens de traitement desdites listes, liste d'identifiants d'équipements, liste d'identifiants de comportements, liste d'associations entre un identifiant d'équipements et un identifiant de comportements.



$$\begin{cases}
 L_{ID_A} = [IdB, IdC, \dots, IdF, IdH] \\
 L_{CA} = [RCA_1, RCA_2, \dots, RCA_k, \dots, RCA_n] \\
 RCA_k = [CA_1, CA_2, \dots, CA_p] \\
 L_{IC_A} = [[IdB[RCA_1]]; [IdC[RCA_k]]]; \dots
 \end{cases}$$

FIG.1

**FIG.2a**

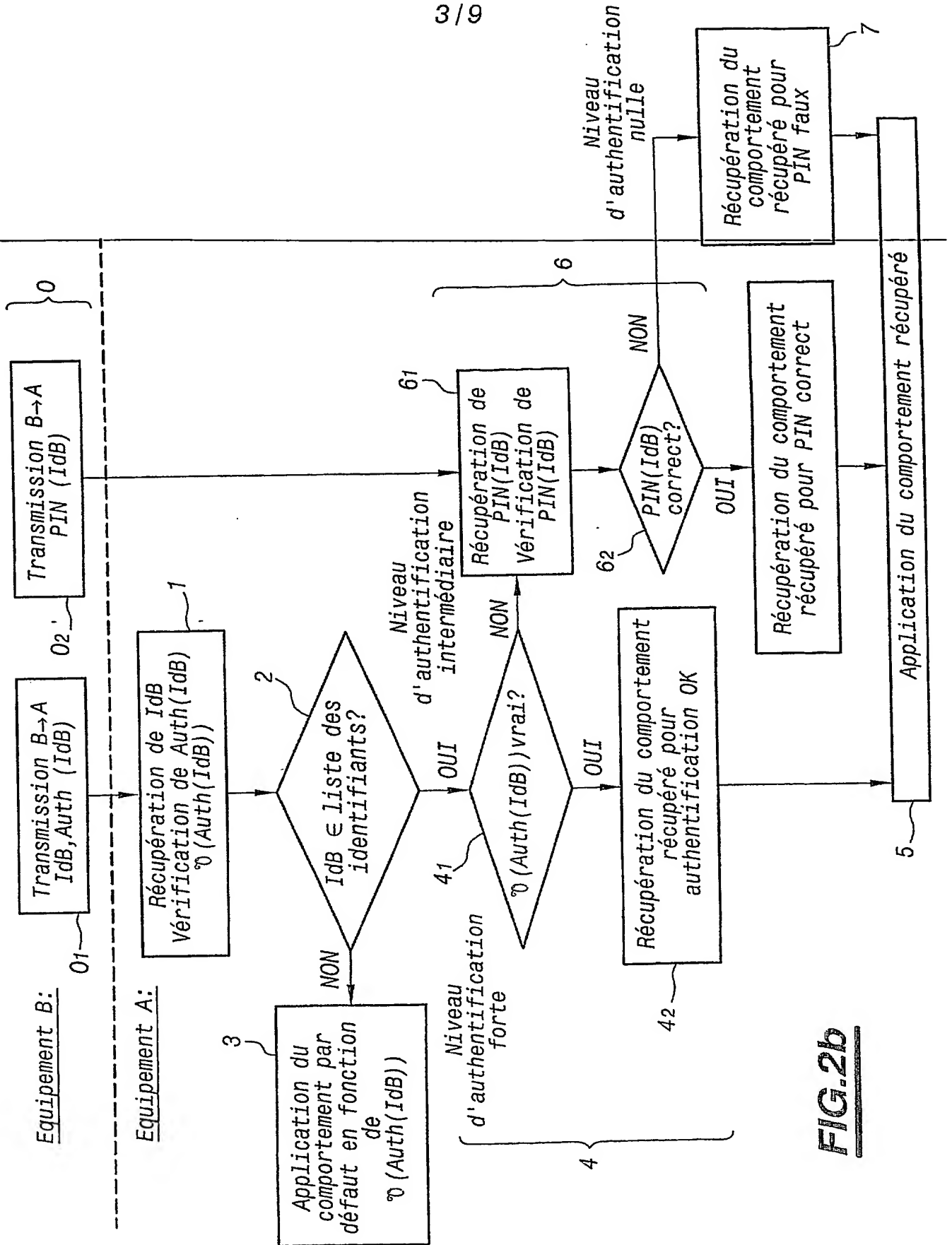


FIG.2b

Equipement A

$$\begin{aligned}
 L_ID_A &= [IdB, IdC, \dots, IdF, IdH] \\
 L_C_A &= [RCA_1, RCA_2, \dots, RCA_k, \dots, RCA_n] \\
 RCA_k &= [CA_1, CA_2, \dots, CA_p] \\
 L_IC_A &= [[IdB[RCA_1]], [IdC[RCA_k]], \dots]
 \end{aligned}$$
Equipement B

$$\begin{aligned}
 L_ID_B &= [IdA, IdD, IdE] \\
 L_C_B &= [RCB_1, RCB_2, \dots, RCB_h, \dots, RCB_r] \\
 RCB_h &= [CB_1, CB_2, \dots, CB_q] \\
 L_IC_B &= [[IdA[RCB_2]], [IdD[RCB_1]], \dots]
 \end{aligned}$$
FIG.2cEquipement A (Terminal)

$$\begin{aligned}
 L_ID_A &= [IdB, IdC, \dots, IdF, IdH] \\
 L_C_A &= [RCA_1, RCA_2, \dots, RCA_k, \dots, RCA_n] \\
 RCA_k &= 010010110 \\
 L_IC_A &= [[IdB[RCA_1]], [IdC[RCA_2]], \dots] \\
 &\quad \underbrace{(010010)}_{(01001)} \quad \underbrace{(01001)}_{(01001)}
 \end{aligned}$$
Equipement B (Carte)

$$\begin{aligned}
 L_ID_B &= [IdA, IdD, IdE] \\
 L_C_B &= [RCB_1, RCB_2, \dots, RCB_h, \dots, RCB_r] \\
 RCB_h &= 1001010 \\
 L_IC_B &= [[IdA[RCB_2]], [IdD[RCB_1]], \dots] \\
 &\quad \underbrace{(01001)}_{(01001)} \quad \underbrace{(0100)}_{(0100)}
 \end{aligned}$$
FIG.2d

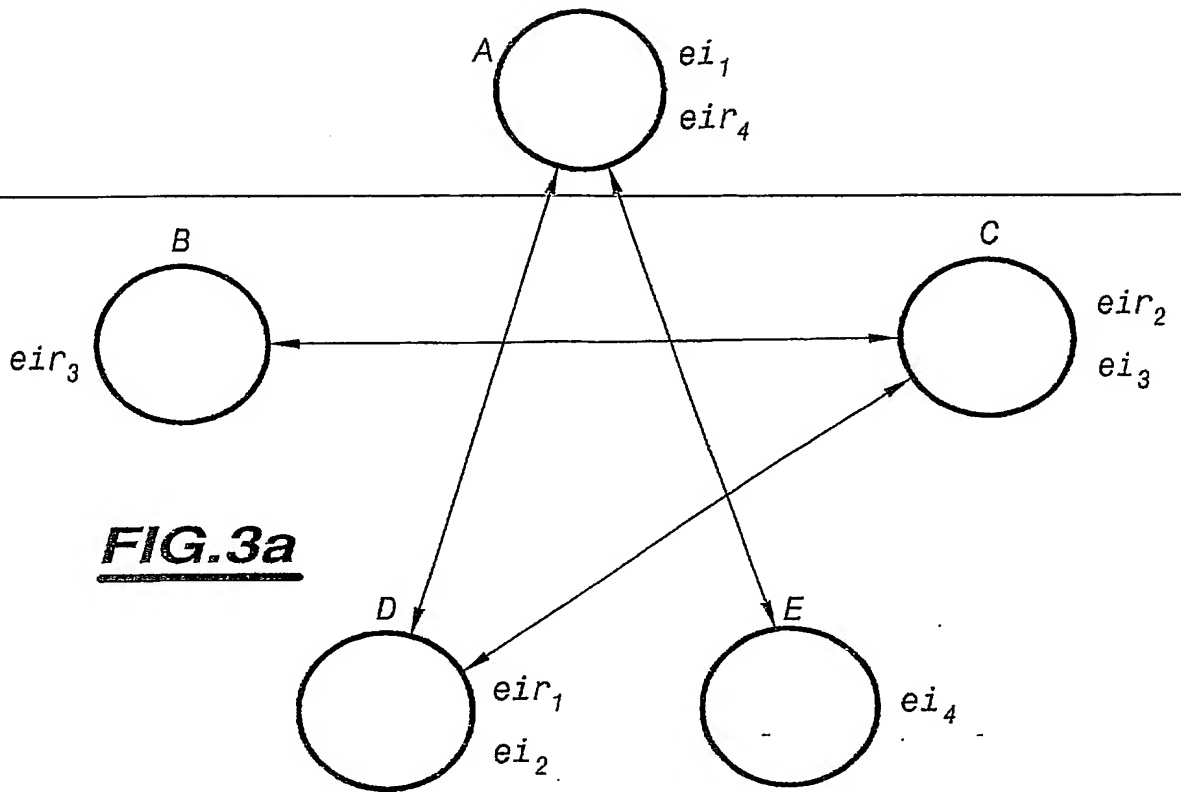


FIG. 3a

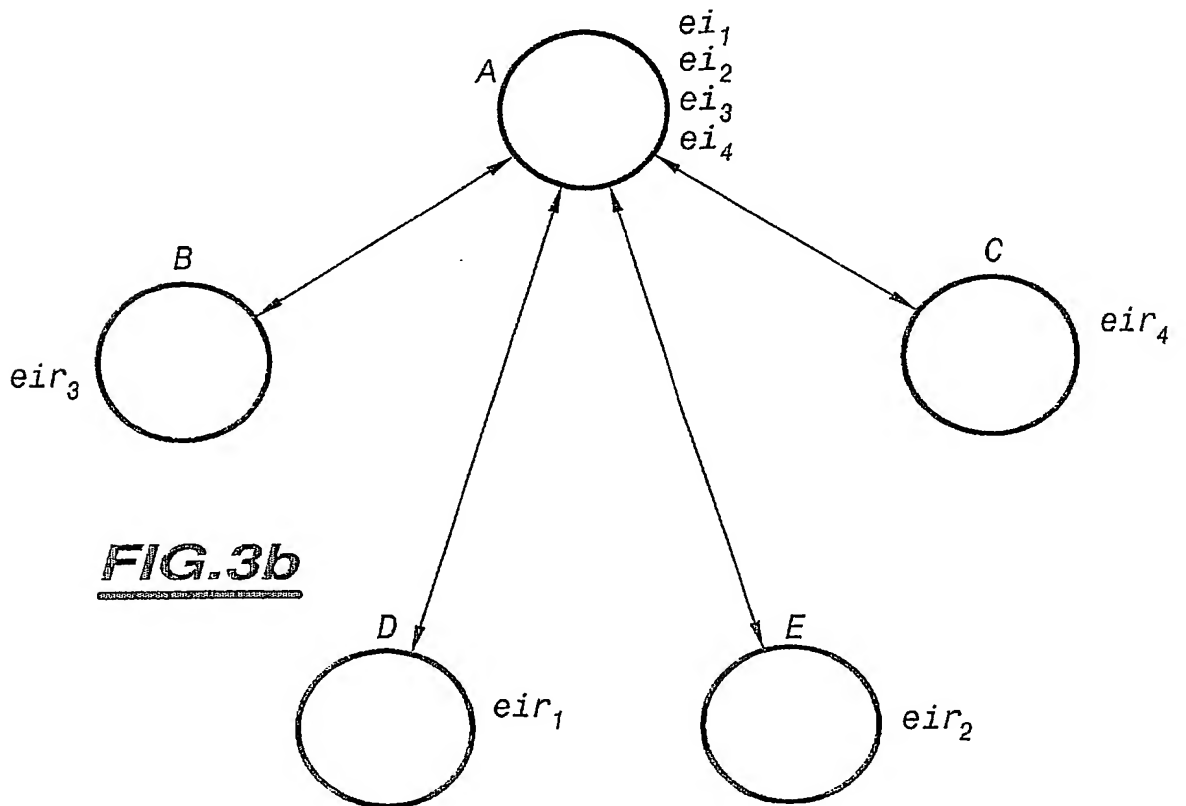
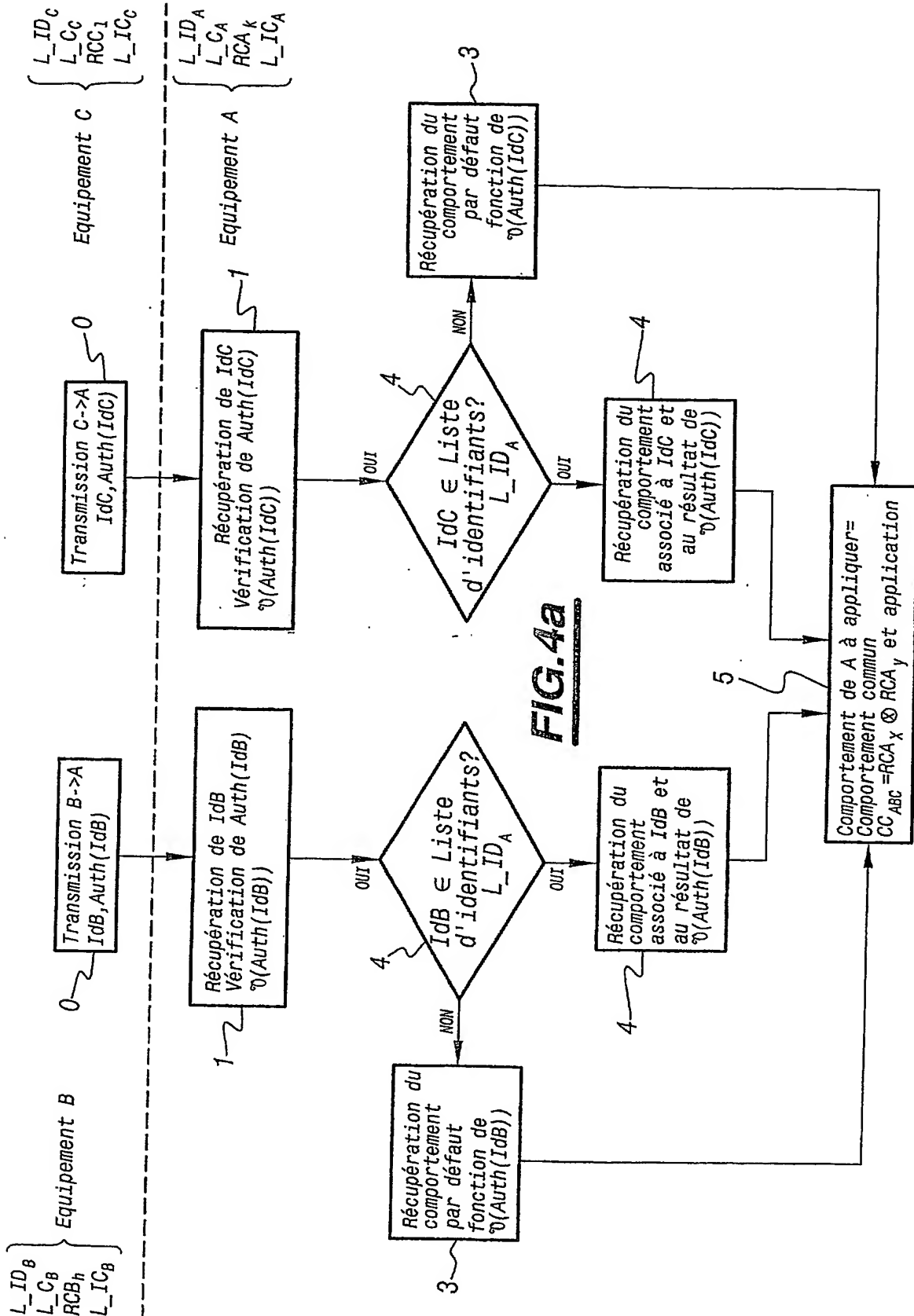


FIG. 3b



Equipment A

$L_ID_A = [IdB, IdC, \dots, IdF, IdH]$
 $L_C_A = [RCA_1, RCA_2, \dots, RCA_k, \dots, RCA_n]$
 $RCA_k = [CA_1, CA_2, \dots, CA_p]$
 $L_IC_A = [[IdB[RCA_1]], [IdC[RCA_k]], \dots]$

Equipment B

$L_ID_B = [IdA, IdC, \dots, IdE]$
 $L_C_B = [RCB_1, RCB_2, \dots, RCB_h, \dots, RCB_r]$
 $RCB_h = [CB_1, CB_2, \dots, CB_q]$
 $L_IC_B = [[IdA[RCB_2]], [IdD[RCB_1]], \dots]$

Equipment C

$L_ID_C = [IdA, IdB, \dots, IdF]$
 $L_C_C = [RCC_1, RCC_2, \dots, RCC_1, \dots, RCC_s]$
 $RCC_1 = [CC_1, CC_2, \dots, CC_o]$
 $L_IC_C = [[IdA[RCC_1]], [IdB[RCC_1]], \dots]$

FIG.4b

$$L_{IC_A} = [[IdB[RCA_1]]; [IdC[RCA_p]]]$$

$$CC_{ABC} = RCA_1 \cap RCA_p$$

FIG.4c

$$L_{IC_A} = [[IdB, [RCA_1]]; [IdC[RCA_p]]]$$

$$\quad \quad \quad \overbrace{b=(010010)} \quad \overbrace{c=(010010)}$$

$$CC_{ABC} = b \cap c = \text{bitand}(b, c)$$

FIG.4d

$$L_{IC_A} = [[IdB[RCA_1]]; [IdC[RCA_p]]]$$

$$CC_{ABC} = RCA_1 \cup RCA_p$$

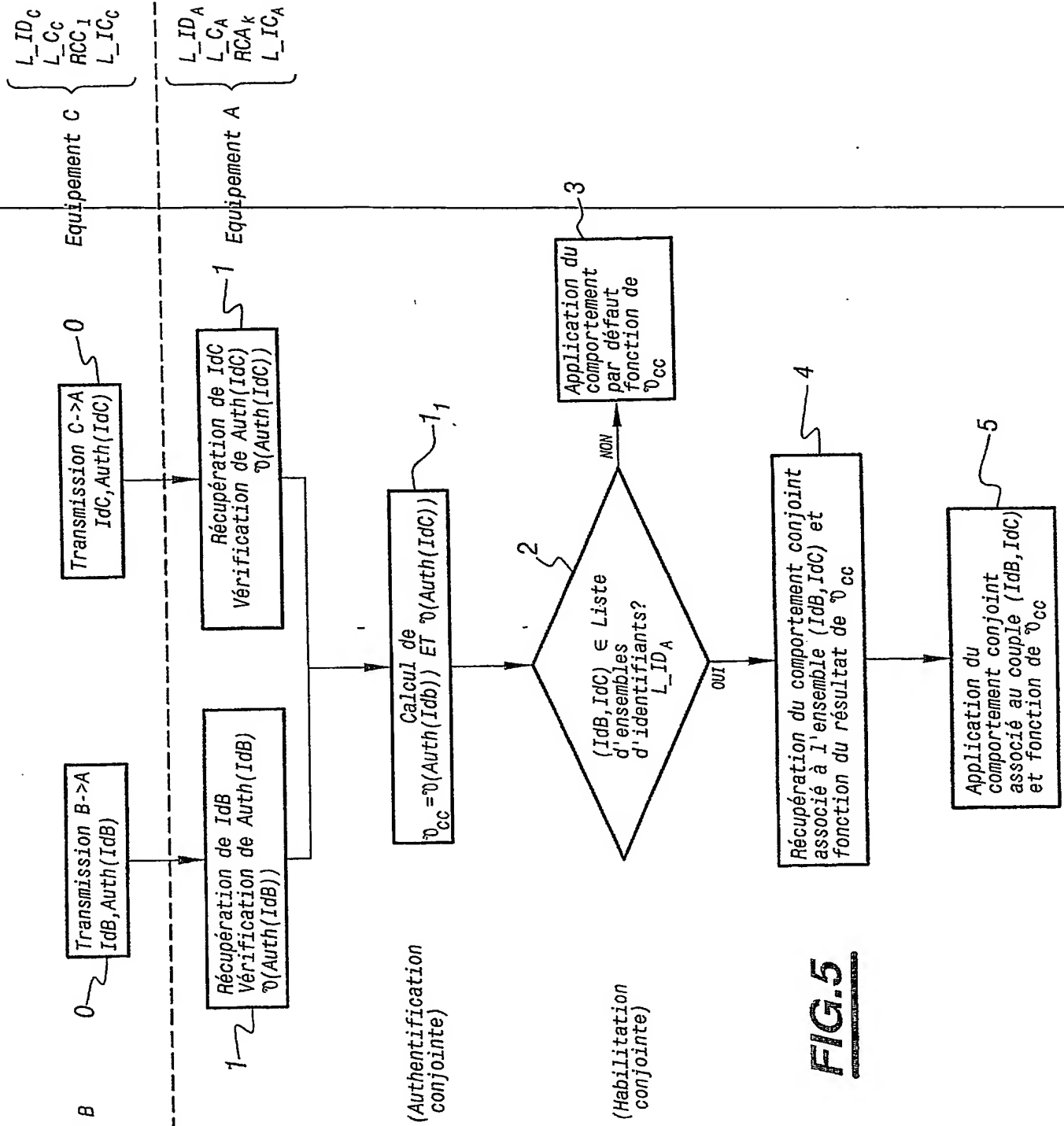
FIG.4e

$$L_{IC_A} = [[IdB[RCA_1]]; [IdC[RCA_p]]]$$

$$\quad \quad \quad \overbrace{b=(010010)} \quad \overbrace{c=(010011)}$$

$$CC_{ABC} = b \cup c = \text{bitor}(b, c) = 010011$$

FIG.4f

**FIG.5**

DÉPARTEMENT DES BREVETS

26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08

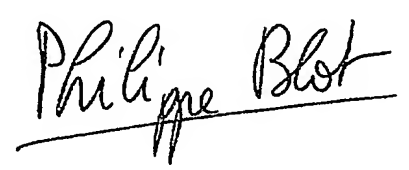
Téléphone : 01 53 04 53 04 Télécopie : 01 42 94 86 54

DÉSIGNATION D'INVENTEUR(S) Page N° 1/2.

(Si le demandeur n'est pas l'inventeur ou l'unique inventeur)

Cet imprimé est à remplir lisiblement à l'encre noire

08 113 W /200599

Vos références pour ce dossier (facultatif)		BFF 01/0499	
N° D'ENREGISTREMENT NATIONAL		020 7984	
TITRE DE L'INVENTION (200 caractères ou espaces maximum)			
Protocole d'adaptation du degré d'interactivité entre équipements informatiques interlocuteurs soumis à un dialogue interactif.			
LE(S) DEMANDEUR(S) :			
VIACCESS			
DESIGNE(NT) EN TANT QU'INVENTEUR(S) : (Indiquez en haut à droite «Page N° 1/1» S'il y a plus de trois inventeurs, utilisez un formulaire identique et numérotez chaque page en indiquant le nombre total de pages).			
Nom		BECKER	
Prénoms		Claudia	
Adresse	Rue	47, rue Vasselot	
	Code postal et ville	35000 RENNES	FRANCE
Société d'appartenance (facultatif)			
Nom		CODET	
Prénoms		André	
Adresse	Rue	Appartement 4757 1, Chemin de Torigné	
	Code postal et ville	35200 RENNES	FRANCE
Société d'appartenance (facultatif)			
Nom		FEVRIER	
Prénoms		Pierre	
Adresse	Rue	3, rue des Trois Pignons	
	Code postal et ville	35250 SAINT SULPICE LA FORET	FRANCE
Société d'appartenance (facultatif)			
DATE ET SIGNATURE(S) DU (DES) DEMANDEUR(S) OU DU MANDATAIRE (Nom et qualité du signataire)		Paris, le 26 juin 2002	
		Ph. BLOT n° 98-0404	
			

reçu le 05/09/02



BREVET D'INVENTION

CERTIFICAT D'UTILITÉ

Code de la propriété intellectuelle - Livre VI



DÉPARTEMENT DES BREVETS

26 bis, rue de Saint Pétersbourg

75800 Paris Cedex 08

Téléphone : 01 53 04 53 04 Télécopie : 01 42 94 86 54

DÉSIGNATION D'INVENTEUR(S) Page N° 2 / 2.

(Si le demandeur n'est pas l'inventeur ou l'unique inventeur)

Cet imprimé est à remplir lisiblement à l'encre noire

08 113 7266

Vos références pour ce dossier

(facultatif)

BFF 01/0499

N° D'ENREGISTREMENT NATIONAL

020 7914

TITRE DE L'INVENTION (200 caractères ou espaces maximum)

Protocole d'adaptation du degré d'interactivité entre équipements informatiques interlocuteurs soumis à un dialogue interactif.

LE(S) DEMANDEUR(S) :

VIACCESS

DESIGNE(NT) EN TANT QU'INVENTEUR(S) : (Indiquez en haut à droite «Page N° 1/1» S'il y a plus de trois inventeurs utilisez un formulaire identique et numérotez chaque page en indiquant le nombre total de pages).

Nom

GUILONNET

Prénoms

Chantal

Adresse

Rue

1, rue des Noés

Code postal et ville

35510 CESSON SEVIGNE

FRANCE

Société d'appartenance (facultatif)

Nom

Prénoms

Adresse

Rue

Code postal et ville

Société d'appartenance (facultatif)

Nom

Prénoms

Adresse

Rue

Code postal et ville

Société d'appartenance (facultatif)

DATE ET SIGNATURE(S)

DU (DES) DEMANDEUR(S)

OU DU MANDATAIRE

(Nom et qualité du signataire)

Paris, le 26 juin 2002

Ph. BLOT
n° 98-0404

Philippe Blot

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☒ FADED TEXT OR DRAWING
- ☒ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☒ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☒ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.